



Weight distributions of cosets of 2-error-correcting binary BCH codes, extended or not

Pascale Charpin

► To cite this version:

Pascale Charpin. Weight distributions of cosets of 2-error-correcting binary BCH codes, extended or not. [Research Report] RR-2228, INRIA. 1994. inria-00074442

HAL Id: inria-00074442

<https://hal.inria.fr/inria-00074442>

Submitted on 24 May 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Weight Distributions of Cosets of 2-Error-Correcting Binary BCH Codes, Extended or not

Pascale CHARPIN

N° 2228

Mars 1994

PROGRAMME 2

Calcul symbolique,
programmation
et génie logiciel

R
*apport
de recherche*

1994

Enumérateurs des poids des translatés des
codes BCH primitifs binaires 2-correcteurs,
étendus ou non

Weight distributions of cosets of
2-error-correcting binary BCH codes,
extended or not

PASCALE CHARPIN ¹

¹ INRIA, projet CODES, Domaine de Voluceau, Rocquencourt, BP 105,
78153 Le Chesnay Cedex, FRANCE.

Résumé

La détermination des énumérateurs des poids des translatés des codes linéaires est un sujet de recherche important en théorie algébrique des codes. Les problèmes rencontrés intéressent tous les spécialistes des structures finies (designs, géométrie finie, corps finis...). D'autre part, lorsque l'on connaît les premiers coefficients des énumérateurs des poids des translatés d'un code, on dispose d'un outil fiable pour évaluer les performances du code. Nous étudions ici les codes BCH 2-correcteurs binaires primitifs, étendus ou non.

Nous notons B le code BCH 2-correcteur binaire de longueur $2^m - 1$ et \hat{B} le code B étendu. Lorsque m est impair, le code B a des propriétés remarquables et il est bien connu que les distributions de poids des translatés de B sont au nombre de quatre. Notre principal résultat est obtenu lorsque m est pair. Dans un article récent, CAMION, COURTEAU et MONTPETIT donnaient explicitement les énumérateurs des poids des translatés des codes BCH 2-correcteurs de longueur 15, 63 et 255. Dans tous les cas ils trouvaient huit énumérateurs distincts. Ceci permettait de conjecturer que les énumérateurs des poids des BCH 2-correcteurs sont au nombre de huit, pour toute longueur $2^m - 1$, m pair. Nous montrons que cette conjecture est vraie. Nous donnons explicitement les matrices des distances des codes B et \hat{B} , quelque soit m .

Outre le résultat, de type combinatoire sur le nombre d'énumérateurs des poids des translatés, nous avons voulu donner une expression formelle nouvelle de ces énumérateurs. Tout code C qui est la réunion d'un translaté $x + \hat{B}$ avec \hat{B} lui-même est un code linéaire binaire, dont le dual est un sous-code du code de Reed et Muller d'ordre 2. Pour chaque type de translaté, nous avons calculé le polynôme des poids de C^\perp et nous obtenons ainsi, en utilisant la transformée de MCWILLIAMS, une expression de l'énumérateur du translaté correspondant $x + \hat{B}$, ne dépendant que de m .

Dans ce rapport sont rassemblés:

1. L'article résumé ci-dessus, qui est à paraître dans les *IEEE Transactions on Information Theory* (pages 3-35).
2. Quelques résultats numériques: toutes les distributions de poids en longueur 15, 16, 31 et 32 ; les matrices des distances pour des longueurs plus élevées (pages 36 et suivantes).

Weight distributions of cosets of 2-error-correcting binary BCH codes, extended or not ²

PASCALE CHARPIN

Abstract

Let B be the binary 2-error-correcting BCH code of length $2^m - 1$ and let \hat{B} be the extended code of B . We give formal expressions of weight distributions of the cosets of the codes \hat{B} only depending on m . We can then deduce the weight distributions of the cosets of B . When m is odd, it is well-known that there are four distinct weight distributions for the cosets of B . So our main result is about the even case. In a recent paper, CAMION, COURTEAU and MONTPETIT observe that for the lengths 15, 63 and 255 there are eight distinct weight distributions. We prove that this property holds for the codes \hat{B} and B for all even m .

Index terms – BCH-codes, weight distribution of cosets, quadratic boolean functions, group algebra.

1 Introduction

In this paper we treat only primitive binary codes. Thus the length of the codes we consider will be either $n = 2^m - 1$ or $N = 2^m$, $m > 2$. The BOSE-CHAUDHURI-HOCQUENGHEM (BCH) codes will be always narrow-sense binary BCH-codes. The *distance* and the *weight* will always be the HAMMING distance and the HAMMING weight. References on coding theory are generally to be found in [23]. In order to explain the context of our work, we first recall some general properties; for more details the reader can refer to [18] and [27].

Let E be a linear code of length v and minimal distance d . Then E is a so-called e -error-correcting code with $e = \lfloor \frac{d-1}{2} \rfloor$. Let t be the number of distinct non-zero weights in the dual E^\perp of E ; t is called the *external distance* of the code E , since t is greater than or equal to the *covering radius* ρ of the code E . Recall that

$$\rho = \max_{x \in L} \min \{ \omega(x + c) \mid c \in E \}, \quad L = \mathbb{F}_2^v,$$

where $\omega(x)$ is the weight of the codeword x . The code E is said to be *perfect* if $\rho = e$ and *quasiperfect* if $\rho = e + 1$. The *distance matrix* of the code E is the $2^v \times (v + 1)$ matrix $B(E)$ whose (x, j) -entry is

$$B(x, j) = \text{card} \{ y \in x + E \mid \omega(y) = j \}, \quad x \in \mathbb{F}_2^v.$$

It was shown by DELSARTE that the distance matrix of a code with a given weight distribution is uniquely determined by its first $t + 1$ columns. Moreover, only the u distinct rows of $B(E)$ are significant, which give the distinct weight enumerators of the cosets of E . The weight distributions of the cosets of E can be calculated from the *reduced distance matrix* of E , in fact a $u \times (t + 1)$ matrix. The code E is said to be

² To appear in IEEE-Transactions on Information Theory

completely regular if each row of $B(E)$, labelled by x , only depends on the minimum weight of $x + E$. *Uniformly packed* codes were introduced by SEMAKOV et al. [26]. Another definition was given by VAN-TILBORG[27]: the code E is said to be *uniformly packed* if and only if $t = e + 1$. A more general definition was given by BASSALYGO et al. in [2].

Any 2-error-correcting BCH code of length $2^m - 1$ is quasiperfect [21], so that its covering radius equals 3. Moreover the weight enumerator of its dual is known [22]. Its external distance is 3 when m is odd; it is 5 when m is even. So when m is odd the 2-error-correcting BCH codes are uniformly packed and their distance matrices are known [2]. When m is even the 2-error-correcting BCH codes are not uniformly packed nor completely regular.

An application of the theory of *partition designs* [8][10] to the study of distance matrices of linear codes is given in [9]. The introduction of the *combinatorial matrix* of the code improves significantly the effective computation of the distance matrix. Thus CAMION, COURTEAU and MONTPETIT obtain the distance matrices of the 2-error-correcting BCH codes of lengths 15, 63 and 255. They observe that in these three cases there are eight distinct weight distributions. They asked for a theoretical explanation of their observations which is the aim of our paper. Our main result is that for m even there are eight distinct weight distributions for the cosets of any 2-error-correcting extended BCH codes of length 2^m ; this property also holds for the 2-error-correcting BCH codes of length $2^m - 1$, m even. Moreover we give the weight distributions of the cosets of all 2-error-correcting extended BCH codes, for the even and for the odd case. Each weight enumerator is given as the MAC WILLIAMS transform of a polynomial, the coefficients of which only depend on m . Simple formulae allow us to obtain the weight distributions of the cosets of a 2-error-correcting BCH code from those of its extension.

The paper is organized as follows. In Section 2, we give some definitions and properties, considering our point of view. We will study the cosets of extended BCH codes; these codes are considered in the group algebra $\mathcal{A} = K[\{G, +\}]$, where K and G are respectively the finite fields of order 2 and 2^m . We show how the product in the algebra becomes an interesting tool for our purpose. We want to obtain the weight enumerators of the codes $E = D \cup \hat{B}$ (or equivalently the weight enumerator of E^\perp), where \hat{B} is the extended BCH-code and D one of its cosets. For this reason we present the code \hat{B}^\perp as a union of some special cosets of the Reed-Muller code of order 2.

The powers of the radical P of \mathcal{A} are the Reed-Muller codes. In Section 3, we study the weight enumerators of the cosets $y + \hat{B}$ of the code \hat{B} , for $y \in P^i \setminus P^{i+1}$, in the three cases $i = 0, 1$ and 2 (by convention $P^0 = \mathcal{A}$). The differences between the three cases are essentially due to the different values of the products $y\hat{B}^\perp$. We study in Section 4 the cosets of the BCH-codes themselves. Let us denote by B any 2-error-correcting BCH-code. We show how every weight enumerator of a coset of B can be obtained from two distinct weight enumerators of cosets of \hat{B} . In Section 5 we give all distance matrices.

The weight enumerators we calculate here are formal objects whose coefficients are formal expressions depending on the length 2^m of the codes. We have needed a computer for the calculation and the simplification of every formulae given in Tables 3 to 9. Some proofs are obtained by solving equations involved by the first *moments*

of some weight distributions; in particular the coefficients of distances matrices are obtained in this way. All these manipulations were made by means of the symbolic computation software Maple.

Main notation

- The length of the cyclic codes is $n = 2^m - 1$; then the length of the extended cyclic codes is $N = 2^m$.
- $\mathbf{G} = GF(2^m)$ and $\mathbf{K} = GF(2)$; $\mathbf{G}^* = \mathbf{G} \setminus \{0\}$.
- α is a primitive root of the finite field \mathbf{G} .
- \mathcal{A} is the modular algebra $\mathbf{K}[\{\mathbf{G}, +\}]$.
- $R(i, m)$ is the Reed-Muller (RM) code of order i and length 2^m .
- P^j , $j \in [1, m]$, is the j th power of the radical P of \mathcal{A} , identified to $R(m - j, m)$.
- The all-one vector in \mathcal{A} is denoted by $\mathbf{1}$ and identified to $(1, \dots, 1) \in \mathbf{K}^N$.
- $S(y)$ is the syndrome of a given codeword y (see (11) and (23)).
- $\omega(x)$ is the Hamming weight of the codeword x .
- If E is a linear code, its dual is denoted by E^\perp ; the usual dot product is denoted by $\langle x, y \rangle$ where x and y are any vectors in the ambient space.
- B is the binary 2-error-correcting BCH code of length n .
- \hat{B} is the extension of B ; it is a binary extended cyclic code of length N .
- γ_i 's and δ_i 's are weights of \hat{B}^\perp respectively for m odd and m even (see (17)).
- C_y is the linear code $\hat{B} \cup (y + \hat{B})$, where $y \notin \hat{B}$.

2 Preliminaries

As usual a binary cyclic code of length n is an ideal of the quotient algebra $\mathbf{K}[Z]/(Z^n - 1)$, where $\mathbf{K} = GF(2)$. Such an ideal is always principal; the roots of its generator polynomial are the zeros of the code. A linear code of length n , dimension k and minimal distance d is said to be an $[n, k, d]$ code.

2.1 The 2-error-correcting BCH codes, \hat{B} and B

Let $n = 2^m - 1$ and $i \in [0, n]$; we denote by $cl(i)$ the cyclotomic coset of $i \bmod n$;

$$cl(i) = \{ i, 2i \bmod n, \dots, 2^{m-1}i \bmod n \}. \quad (1)$$

Definition 1 *The narrow-sense 2-error-correcting BCH code is the cyclic code of length n whose zero set is :*

$$\bigcup_{i \in I} \{ \alpha^i \} \quad , \quad I = cl(1) \cup cl(3) \quad ,$$

where α is a primitive root of $GF(2^m)$. This code will be denoted by B ; it is an $[n, 2^m - 2m - 1, 5]$ code.

The dual of B , denoted by B^\perp , is the cyclic code of length n whose zero set is :

$$\bigcup_{i \in I} \{ \alpha^i \} , \quad I = [0, n-1] \setminus \{ cl(n-1), cl(n-3) \} .$$

Let E be a binary linear code of length n . Its extension is the code \hat{E} obtained by adding an overall parity-check:

$$(c_0, \dots, c_n) \in E \implies (c_\infty, c_0, \dots, c_n) \in \hat{E} \text{ where } c_\infty = \sum_{i=0}^n c_i .$$

If the code E is $[n, k, d]$, then the code \hat{E} is $[n+1, k, d']$, with $d' \geq d$. If d is odd then $d' = d+1$. Let H be the parity check matrix of E ; thus the parity check matrix of \hat{E} is as follows:

$$\hat{H} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 0 & & & \\ \vdots & H & & \\ 0 & & & \end{bmatrix}$$

Definition 2 The extended binary 2-error-correcting BCH code of length $N = 2^m$ is the code

$$\hat{B} = \{ (x_\infty, x_0, \dots, x_n) \mid (x_0, \dots, x_n) \in B , x_\infty = \sum_{i=0}^n x_i \} .$$

The code \hat{B} is $[N, 2^m - 2m - 1, 6]$. Let us denote by $\mathbf{1}$ the all-one vector of length N . The dual of \hat{B} can be defined as follows:

$$\hat{B}^\perp = L \cup (\mathbf{1} + L) \text{ where } L = \{ (0, x_0, \dots, x_n) \mid (x_0, \dots, x_n) \in B^\perp \} . \quad (2)$$

The weight distributions of the codes B^\perp are given in [23], p.452 and 453. In accordance with (2), the weight distributions of the codes \hat{B}^\perp are easily obtained; they are presented in Tables 1 and 2.

Consider the cosets $x + R(1, m)$, where x is an element of $R(2, m) \setminus R(1, m)$ ($R(i, m)$ is the Reed-Muller code of length 2^m and order i). These cosets are in one-to-one correspondence with *symplectic forms*; the *rank* of a given symplectic form uniquely determines the weight distribution of the corresponding coset (see [23], Chapter 15). The code \hat{B}^\perp consists of the code $R(1, m)$ itself and of some of its cosets of high rank (more details can be found in Section 2.5). When m is odd the rank of any coset equals $m-1$ and we will say that the cosets are of type (I). When m is even the rank equals m or $m-2$ and will say the the cosets are respectively of type (II) or (III).

2.2 Mac Williams transform and cosets of \hat{B}

In this paragraph we recall some formulae we need later for the computation of weight distributions. The extended 2-error-correcting BCH code of length 2^m over $GF(2)$ will always be denoted by \hat{B} .

Number of cosets	Number of words in a coset	weights	Total number of words
(I) : $2^m - 1$	2^{m-1}	$2^{m-1} - 2^{(m-1)/2}$	$(2^m - 1)2^{m-1}$
	2^{m-1}	$2^{m-1} + 2^{(m-1)/2}$	$(2^m - 1)2^{m-1}$
	2^m	2^{m-1}	$2^{2m} + 2^m - 2$
$R(1, m)$	$2^{m+1} - 2$	2^{m-1}	
	1	2^m	1
	1	0	1

Table 1: Weight distribution of \hat{B}^\perp , m odd

Number of cosets	Number of words in a coset	weights	Total number of words
(II) : $\frac{2(2^m-1)}{3}$	2^m	$2^{m-1} - 2^{m/2-1}$	$2^{m+1}(2^m - 1)/3$
	2^m	$2^{m-1} + 2^{m/2-1}$	$2^{m+1}(2^m - 1)/3$
(III) : $\frac{2^m-1}{3}$	2^{m-2}	$2^{m-1} - 2^{m/2}$	$2^{m-2}(2^m - 1)/3$
	2^{m-2}	$2^{m-1} + 2^{m/2}$	$2^{m-2}(2^m - 1)/3$
	$3 \cdot 2^{m-1}$	2^{m-1}	$2^{2m-1} + 3 \cdot 2^{m-1} - 2$
$R(1, m)$	$2^{m+1} - 2$	2^{m-1}	
	1	2^m	1
	1	0	1

Table 2: Weight distribution of \hat{B}^\perp , m even

Theorem 1 ([23], pp.127-132) *Let E be a linear binary code of length v . We define its weight enumerator:*

$$W_E(X, Y) = \sum_{i=0}^v A_i X^{v-i} Y^i, \quad A_i = |\{c \in E \mid \omega(c) = i\}|,$$

where $|H|$ denotes the number of elements of some set H . Then the weight enumerator of the dual code E^\perp is

$$W_{E^\perp}(X, Y) = \frac{1}{|E|} W_E(X + Y, X - Y). \quad (3)$$

Let $A'_i = |\{c \in E^\perp \mid \omega(c) = i\}|$; denote by k the dimension of E^\perp . If the weight enumerator of E is known, then the A'_i 's can be calculated by means of the following identities:

$$\forall j, j \in [0, v] : \sum_{i=0}^{v-j} \binom{v-i}{j} A'_i = 2^{k-j} \sum_{i=0}^j \binom{v-i}{v-j} A_i. \quad (4)$$

Let $D = y + E$ be a coset of E , where y is not in E . Since E is a linear binary code, it is clear that the code $E \cup (y + E)$ is also linear. If the weight polynomial

of its dual code and of E^\perp are known, then one can obtain the weight enumerator of D . We shall use this method to compute the weight enumerators of the cosets of the codes \hat{B} .

Lemma 1 Let $N = 2^m$, $y \in K^N$, $y \notin \hat{B}$; set $C_y = \hat{B} \cup (y + \hat{B})$. By extending the definition given in Theorem 1 to nonlinear codes, we denote by $W_{y+\hat{B}}(X, Y)$ the weight enumerator of the coset $y + \hat{B}$.

Then $C_y^\perp \subset \hat{B}^\perp$, $\dim C_y^\perp = \dim \hat{B}^\perp - 1 = 2m$, and

$$W_{y+\hat{B}}(X, Y) = \frac{1}{2^{2m+1}} \left(2W_{C_y^\perp}(X+Y, X-Y) - W_{\hat{B}^\perp}(X+Y, X-Y) \right). \quad (5)$$

Proof: Recall that $\dim \hat{B} = N - (2m+1)$. By definition we have $\hat{B} \subset C_y$ which yields $C_y^\perp \subset \hat{B}^\perp$ and $\dim C_y = \dim \hat{B} + 1 = 2^m - 2m$. Thus $\dim C_y^\perp = 2^m - (2^m - 2m) = 2m$. Applying (3), we have

$$W_{C_y}(X, Y) = \frac{1}{2^{2m}} W_{C_y^\perp}(X+Y, X-Y).$$

But, by definition, $W_{C_y}(X, Y) = W_{y+\hat{B}}(X, Y) + W_{\hat{B}}(X, Y)$, which yields

$$W_{y+\hat{B}}(X, Y) = \frac{1}{2^{2m}} W_{C_y^\perp}(X+Y, X-Y) - \frac{1}{2^{2m+1}} W_{\hat{B}^\perp}(X+Y, X-Y).$$

□

2.3 The codes \hat{B} in the algebra $\mathcal{A} = K[G]$

In order to study the codes C_y , we will consider the codes \hat{B} in the group algebra $\mathcal{A} = K[\{G, +\}]$, where $K = GF(2)$ and $G = GF(2^m)$. The main interest of doing so is in the use of the multiplication of the algebra as we will show in the next paragraph.

The group algebra \mathcal{A} is the set of formal polynomials

$$x = \sum_{g \in G} x_g X^g, \quad x_g \in K,$$

with $0 = \sum_{g \in G} 0 X^g$, $I = \sum_{g \in G} X^g$,

$$x + y = \sum_{g \in G} x_g X^g + \sum_{g \in G} y_g X^g = \sum_{g \in G} (x_g + y_g) X^g,$$

and

$$xy = \sum_{g \in G} x_g X^g \sum_{g \in G} y_g X^g = \sum_{h \in G} \left(\sum_{g \in G} x_g y_{g+h} \right) X^h, \quad (6)$$

x and y any element in \mathcal{A} . A linear code of \mathcal{A} is a K -subspace of \mathcal{A} . Let E be such a code; then its dual code is:

$$E^\perp = \{ y \in \mathcal{A} \mid \langle x, y \rangle = 0, \text{ for all } x \in E \} \text{ where } \langle x, y \rangle = \sum_{g \in G} x_g y_g.$$

The algebra \mathcal{A} has only one maximal ideal, which is called its *radical*. The radical of \mathcal{A} is denoted by P and is defined as follows:

$$P = \{ x \in \mathcal{A} \mid \sum_{g \in G} x_g = 0 \} = \{ x \in \mathcal{A} \mid x^2 = 0 \}. \quad (7)$$

Berman proved in [5] that the powers of the radical of \mathcal{A} are the Reed-Muller codes. More precisely:

Theorem 2 *For any j , we denote by P^j the j th power of P ; it is the subspace of \mathcal{A} generated by the products $\prod_{i=1}^j x_i$, $x_i \in P$. One obtains the decreasing sequence of ideals of \mathcal{A} :*

$$\{0\} = P^{m+1} \subset P^m \subset \dots \subset P^2 \subset P,$$

(by convention $P^0 = \mathcal{A}$). Then we have $P^j = R(m-j, m)$, for all $j \in [1, m]$.

From a well-known property of the RM-codes, we have then $(P^j)^\perp = P^{m-j+1}$. In Section 3, we will study the cosets $y + \hat{B}$ with $y \in P^i \setminus P^{i+1}$, successively for $i = 0, 1$ and 2 . We want now to identify precisely the extended cyclic codes in \mathcal{A} that we will use later. More details on properties of the algebra \mathcal{A} and on codes of \mathcal{A} can be found in [13, 14].

Proposition 1 *Let $S = [0, n]$, $n = 2^m - 1$. An extended cyclic code E in \mathcal{A} is uniquely determined by a subset T of S such that $0 \in T$ and T is a union of cyclotomic cosets of 2 modulo n . Let us define for all $s \in S$ and for all $x \in \mathcal{A}$:*

$$\phi_s(x) = \sum_{g \in G} x_g g^s \in G.$$

By convention, $\phi_0(x) = \sum_{g \in G} x_g$. Then we have that

$$E = \{ x \in \mathcal{A} \mid \phi_s(x) = 0, \text{ for all } s \in T \}$$

We say that T is the defining set of the code C .

Definition 3 1) Let $s \in S$; let $\sum_{i=0}^{m-1} s_i 2^i$, $s_i \in \{0, 1\}$, be the binary expansion of s . We denote by $\omega_2(s)$ the 2-weight of s ; that is

$$\omega_2(s) = \sum_{i=0}^{m-1} s_i.$$

The RM-code of length 2^m and order $m - r$ (i.e. the code P^r) is the extended cyclic code with defining-set

$$T(P^r) = \{ s \in S \mid \phi_s(x) = 0 \text{ for } 0 \leq \omega_2(s) < r \}. \quad (8)$$

2) The defining-set of the extended 2-error-correcting BCH code \hat{B} is

$$T(\hat{B}) = \{ 0, cl(1), cl(3) \}. \quad (9)$$

3) The defining-set of the dual \hat{B}^\perp of \hat{B} is

$$T(\hat{B}^\perp) = S \setminus \{ n, cl(n-1), cl(n-3) \}, \quad S = [0, n]. \quad (10)$$

Remark 1: 1 – By definition, an extended cyclic code is a subspace of P . It can be an ideal of \mathcal{A} . For instance RM-codes and BCH-codes are ideals of \mathcal{A} ; a K -subspace E of \mathcal{A} which satisfies $P^j \subset E \subset P^{j-1}$ for some j , is an ideal of \mathcal{A} [13].

2 – It is clear that there is a one-to-one correspondence between the cosets $y + \hat{B}$ of the code \hat{B} and the following elements of G^3 : $\phi_i(y)$, $i = 0, 1, 3$. Indeed, in accordance with (9), the parity check matrix of \hat{B} can be taken to be:

$$\begin{bmatrix} 1 & . & . & . & \dots & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^{3(n-1)} \end{bmatrix}$$

Hence the *syndrome*, say $\mathcal{S}(y)$, of y (or of the coset containing y) is the value of $\hat{H}y^T$ [23, ch. 9]. It is exactly:

$$\mathcal{S}(y) = (\phi_0(y), \phi_1(y), \phi_3(y)) , \quad y \in \mathcal{A} \setminus \hat{B} . \quad (11)$$

As for codewords of cyclic codes, we can define the MATTSON-SOLOMON (MS) polynomial of an extended codeword. For any $x \in P$ the MS-polynomial of x is the following element of $G[Z]$:

$$M_x(Z) = \sum_{s=1}^n \phi_s(x) Z^{n-s} \quad (12)$$

We recall the well-known property [23, p. 239]:

Proposition 2 *Let α be a primitive root of the finite field G . Let $x \in P$. Then for all $k \in [1, n]$, we have $M_x(\alpha^k) = x_{\alpha^k}$. Note that $M_x(0) = \phi_n(x) = x_0 = \sum_{g \in G} x_g$.*

2.4 Multiplication in \mathcal{A}

Proposition 3 *Let $x \in \mathcal{A}$ and $y \in \mathcal{A}$. Then the weight of the product xy satisfies*

$$\omega(xy) = \text{card} \{ h \in G \mid \langle X^h x, y \rangle = 1 \} .$$

Proof: In accordance with (6), we have:

$$\begin{aligned} xy &= \sum_{h \in G} \left(\sum_{g \in G} x_{h+g} y_g \right) X^h \\ &= \sum_{h \in G} \left(\langle X^h x, y \rangle \right) X^h . \end{aligned}$$

Note that $(xy)_0 = \langle x, y \rangle$.

□

Remark 2: The formula above shows that for any $y \in \hat{B}$ and any $x \in \hat{B}^\perp$ the product xy is zero. Indeed \hat{B} and \hat{B}^\perp are ideals of \mathcal{A} – i.e. they are invariant under multiplication by any X^h .

Proposition 4 Any $s \in S$ is identified with its binary expansion (s_0, \dots, s_{m-1}) . Then we define a partial order on S :

$$\forall s, t \in S : s < t \iff \forall i \in [0, m-1] : s_i \leq t_i$$

Let $x \in \mathcal{A}$ and $y \in \mathcal{A}$. Then

$$\forall s \in S : \phi_s(xy) = \sum_{i < s} \phi_i(x) \phi_{s-i}(y) .$$

Proof:

$$\begin{aligned} \phi_s(xy) &= \sum_{g \in G} x_g \sum_{h \in G} y_h (g+h)^s = \sum_{g \in G} x_g \sum_{h \in G} y_h \sum_{i=0}^s \binom{s}{i} g^i h^{s-i} \\ &= \sum_{i=0}^s \binom{s}{i} \sum_{g \in G} x_g g^i \sum_{h \in G} y_h h^{s-i} = \sum_{i < s} \phi_i(x) \phi_{s-i}(y) , \end{aligned}$$

since, by LUCAS's Theorem, $\binom{s}{i} \not\equiv 0 \pmod{2}$ is equivalent to $i < s$ [23, p. 404].

□

Lemma 2 Let $y \in \mathcal{A} \setminus \hat{B}$, $x \in \hat{B}^\perp \setminus P^{m-1}$ and $D = x + P^{m-1}$.

- (i) Assume that $y \in P^2 \setminus \hat{B}$. If $xy = 0$ then $ya = 0$ for all $a \in D$ else $ya = \mathbf{I}$ for all $a \in D$ - i.e. either y is orthogonal to all elements of D or no element of D is orthogonal to y . We will say respectively that $yD = \{0\}$ or that $yD = \{\mathbf{I}\}$.
- (ii) Assume that $y \in \mathcal{A} \setminus P^2$. Then

$$\text{card} \{ a \in D \mid \langle y, a \rangle = 0 \} = \frac{\text{card } D}{2} = 2^m .$$

Proof: In accordance with (8), (9) and (10), it is clear that

$$P^3 \subset \hat{B} \subset P^2 \quad \text{and} \quad P^{m-1} \subset \hat{B}^\perp \subset P^{m-2} .$$

Recall that P^2 is the dual code of P^{m-1} and that $P^m = \{0, \mathbf{I}\}$.

(i) Since $y \in P^2$ then yP^{m-1} is included in P^{m+1} , which is the set $\{0\}$. That implies: $yx = ya$ for all a in D . Since $x \in \hat{B}^\perp$ the product xy is an element of P^m and in this case $\langle x, y \rangle = 0$ is equivalent to $xy = 0$.

(ii) The function $f : u \in P^{m-1} \mapsto \langle y, u \rangle \in K$ is linear. By hypothesis $y \notin (P^{m-1})^\perp$. Then $\dim(\ker f) = \dim(P^{m-1}) - 1 = m$ which yields that the number of $u \in P^{m-1}$ satisfying $\langle y, u \rangle = 0$ equals 2^m . The equality $\langle y, a \rangle = \langle y, x \rangle + \langle y, u \rangle$, $a \in D$, completes the proof.

□

2.5 Description of the codes \hat{B}^\perp

Every coset $x + P^{m-1}$ contains 2^{m+1} codewords. The code \hat{B}^\perp contains 2^{2m+1} codewords; then it consists of 2^m cosets $x + P^{m-1}$ where $x \in P^{m-2}$. In this paragraph we will identify such cosets D with the values $\phi_{n-3}(x)$. Note that $\phi_{n-3}(D)$ is the set $\{\phi_{n-3}(x)\}$, since $\phi_{n-3}(a) = 0$ for all $a \in P^{m-1}$. We also will characterize the codewords of D of a given weight.

Definition 4 Let $\beta = \alpha^{n-3}$ (α is a primitive root of G); we denote by C_β , the linear code of \mathcal{A} whose codewords x satisfy $\phi_s(x) = 0$ if $s \notin \text{cl}(n-3)$.

The code C_β is in fact the irreducible cyclic code, defined by the minimal polynomial of β , viewed in \mathcal{A} . According to (12) we obtain its MS-polynomial

$$M_x(Z) = \text{Tr}(\phi_{n-3}(x)Z^3) \quad \text{for all } x \in C_\beta, \quad (13)$$

where Tr is the trace-function from G to K . By definition the code C_β is included in \hat{B}^\perp . It contains 2^m codewords; its non-zero codewords are not in P^{m-1} , since $\omega_2(n-3) = m-2$ (see (8)). Let x and y be non-zero codewords of C_β . Suppose that $\phi_{n-3}(x) = \phi_{n-3}(y)$. Since ϕ_{n-3} is a linear function, that means that $\phi_s(x+y) = 0$ for all s , which yields $x = y$. We have then proved that the code \hat{B}^\perp consists of the 2^m cosets $x + P^{m-1}$ where $x \in C_\beta$; moreover there is a one-to-one correspondence between the set of such cosets D and the 2^m values $\phi_{n-3}(x)$, $x \in C_\beta$. A special coset is defined by the primitive idempotent of C_β , say τ ; that is the codeword $\tau \in \hat{B}^\perp$ satisfying

$$\phi_n(\tau) = \phi_{n-1}(\tau) = 0 \quad \text{and} \quad \phi_{n-3}(\tau) = 1. \quad (14)$$

Some cosets are equivalent by the shift; we will denote by sh_j the j -shift on codewords of \mathcal{A} ; that is

$$sh_j : \sum_{g \in G} x_g X^g \mapsto \sum_{g \in G} x_g X^{\alpha^j g}. \quad (15)$$

Some properties of elements of the RM-code of order 2 (i.e. of P^{m-2}) are used in the proofs of the following propositions. We only recall the results we need. For more details the reader can refer to [23, chapter 15] and to [11, chapter I].

Let a in P^{m-2} ; then a can be identified to a quadratic boolean function f_a :

$$a = \sum_{g \in G} f_a(g) X^g \quad - \quad \text{i.e.} \quad a_g = f_a(g).$$

The associated symplectic form of f_a is

$$\Psi_a : (u, v) \in G^2 \mapsto \Psi_a(u, v) = f_a(0) + f_a(u) + f_a(v) + f_a(u+v) \in K.$$

The kernel of Ψ_a is defined as follows:

$$\mathcal{E}_a = \{ u \in G \mid \forall v \in G : \Psi_a(u, v) = 0 \}.$$

The set \mathcal{E}_a is a K -subspace of G of dimension $m - 2h$, where $2h$ is the rank of Ψ_a . Let $D = a + P^{m-1}$; then $\Psi_a = \Psi_b$ for all $b \in D$. Moreover the weight distribution of D only depends on h (cf. [23, p. 441]).

Now we can describe precisely the code \hat{B}^\perp :

Proposition 5 Let $n = 2^m - 1$, and let τ be defined by (14). The code \hat{B}^\perp consists of 2^m cosets corresponding to the 2^m codewords of the code C_β .

(i) When m is odd, \hat{B}^\perp consists of P^{m-1} and of the n cosets of type (I) :

$$sh_j(\tau) + P^{m-1}, \quad j \in [0, n[.$$

(ii) Suppose that m is even and set $\nu = n/3$. Let $x^{(1)}$ and $x^{(2)}$ be the elements of C_β satisfying respectively $\phi_{n-3}(x^{(i)}) = \alpha^i$, $i = 1$ and 2 . Then \hat{B}^\perp consists of P^{m-1} , of the ν cosets of type (III)

$$sh_j(\tau) + P^{m-1}, \quad j \in [0, \nu[,$$

of the ν cosets of type (II)

$$sh_j(x^{(1)}) + P^{m-1}, \quad j \in [0, \nu[,$$

and of the ν cosets of type (II)

$$sh_j(x^{(2)}) + P^{m-1}, \quad j \in [0, \nu[.$$

Note that $\phi_{n-3}(sh_j(\tau)) = \alpha^{-3j}$ and that $\phi_{n-3}(sh_j(x^{(i)})) = \alpha^{-3j+i}$, for $i = 1$ and 2 .

Proof: Obviously 3 divides $2^m - 1$ if and only if m is even. Remark that for any $x \in \mathcal{A}$ and any $s \in [1, n-1]$ we have

$$\phi_s(sh_j(x)) = \sum_{g \in \mathbf{G}} x_g (\alpha^j g)^s = \alpha^{js} \phi_s(x). \quad (16)$$

When m is odd, α^3 is a primitive root of \mathbf{G} ; thus the code C_β is equivalent to the simplex code and its codewords are τ and its shifts. Any non-zero codeword has weight 2^{m-1} .

Suppose that m is even and set $s = n-3$ and $n = 3\nu$ in (16). It is clear that for each $x \in C_\beta$ the set $\{sh_j(x)\}_j$ consists of ν distinct elements. Now we must prove that the coset $\tau + P^{m-1}$ is a coset of type (III). Using Proposition 2, (13) and (14) we calculate the associated symplectic form:

$$\begin{aligned} \Psi_\tau(u, v) &= Tr(u^3) + Tr(v^3) + Tr((u+v)^3) = Tr(u^2v + uv^2) \\ &= Tr(v^2(u^4 + u)). \end{aligned}$$

Clearly the equation $u^4 = u$ has exactly four solutions in $GF(2^m)$, when m is even. Thus the dimension of \mathcal{E}_τ equals 2; therefore the rank of Ψ_τ is $m-2$ as the rank of the symplectic forms associated to cosets of type (III) is. Then the remaining cosets corresponding to $x^{(1)}$, $x^{(2)}$ and their shifts are of type (II) (see Table 2).

In all cases the values of ϕ_{n-3} are deduced from (16).

□

Corollary 1 Let $N = 2^m$, m even. Set $\nu = (2^m - 1)/3$. Then the weight enumerator of the code C_β is:

(i) $m \equiv 0 \pmod{4}$: $W(X, Y) = X^N + 2\nu X^{N-\lambda_2} Y^{\lambda_2} + \nu X^{N-\lambda_4} Y^{\lambda_4}$.

(ii) $m \not\equiv 0 \pmod{4}$: $W(X, Y) = X^N + \nu X^{N-\lambda_1} Y^{\lambda_1} + 2\nu X^{N-\lambda_3} Y^{\lambda_3}$.

where $\lambda_1 = 2^{m-1} - 2^{m/2}$, $\lambda_2 = 2^{m-1} - 2^{m/2-1}$, $\lambda_3 = 2^{m-1} + 2^{m/2-1}$, $\lambda_4 = 2^{m-1} + 2^{m/2}$.

Proof: When m is even, it is well-known that the code C_β has only two non-zero weights. The weight enumerator can be obtained as a corollary of Theorem 3 of [19].

We recall that a linear binary code is said to be t -divisible, $t > 1$, if the weights of all its words are divisible by t . If t is not a power of 2, then such a code is equivalent to a degenerate code (in which every symbol is repeated t times).

Since 3 divides n , it is clear from (13) that C_β is 3-divisible. So we can also deduce the weight enumerator of C_β from Table 2 and Proposition 5. Each coset composing \hat{B}^\perp has only one word in C_β , according to Proposition 5. It is sufficient to determine, for any weight λ such that 3 divides λ , the number of such cosets. There are words of weights λ_1 and λ_4 in the cosets of type (III), and words of weights λ_2 and λ_3 in the cosets of type (II). When 4 divides m then 3 divides only λ_2 and λ_4 ; otherwise 3 divides only λ_1 and λ_3 . The number of codewords of weight λ_i in C_β is equal to the number of cosets in \hat{B}^\perp containing codewords of weight λ_i .

□

Proposition 6 Let $a \in P^{m-2} \setminus P^{m-1}$ and $D = a + P^{m-1}$. Let λ be a weight of D such that $\lambda \neq 2^{m-1}$ and suppose that $\omega(a) = \lambda$. We denote by κ the dimension of the kernel of the symplectic form Ψ_a . Then we have:

$$\{ X^g a \mid g \in G \} = \{ b \in D \mid \omega(b) = \lambda \} ,$$

and the cardinality of the set above is $2^{m-\kappa}$. Hence each codeword b of D , of weight different from 2^{m-1} is invariant under 2^κ translations (ie multiplications by an X^g).

Proof: Set $\kappa = m - 2h$. According to Theorem 5 of [23, p.441], we have $2^{2h} = \text{card} \{ b \in D \mid \omega(b) = \lambda \}$, where $\lambda = 2^{m-1} \pm 2^{m-h-1}$. Let u and v in G . By definition, $\Psi_a(u, v) = a_0 + a_u + a_v + a_{u+v}$. Furthermore for any $u \neq 0$

$$(X^u + 1)a = \sum_{v \in G} a_v X^{u+v} + \sum_{v \in G} a_v X^v = \sum_{v \in G} (a_{u+v} + a_v) X^v ,$$

and we have obviously

$$\text{card} \{ X^g a \mid g \in G \} = \frac{\text{card } G}{\text{card} \{ g \in G \mid a = X^g a \}} .$$

An element u is in \mathcal{E}_a if and only if $\Psi_a(u, v) = 0$, for all v . Therefore u is an element of \mathcal{E}_a if and only if

$$(X^u + 1)a = \sum_{v \in G} (a_0 + a_u) X^v = (a_0 + a_u) \mathbf{I} .$$

Assume that u is in \mathcal{E}_a . Since $\omega((X^u + 1)a) \leq 2\omega(a)$ then $(X^u + 1)a = 0$ (equivalently $a_0 = a_u$) in the equality above when $\omega(a) < 2^{m-1}$. This result holds for $\omega(a) > 2^{m-1}$ because P^{m-1} contains the all-one vector \mathbf{I} ; that means that there exists $b \in D$ such that $a = b + \mathbf{I}$ with $\omega(b) < 2^{m-1}$. Obviously $(X^u + 1)a = (X^u + 1)b$.

Conversely $X^u a = a$ implies $a_{u+v} = a_v$ for all v , which means $\Psi_a(u, v) = 0$, for all v .

So we have proved that $X^u a = a$ if and only if $u \in \mathcal{E}_a$. Hence

$$\text{card} \{ g \in G \mid a = X^g a \} = \text{card} \mathcal{E}_a = 2^\kappa,$$

which yields $\text{card} \{ X^g a \mid g \in G \} = 2^{m-\kappa} = 2^{2h}$, completing the proof.

□

3 Weight distributions of cosets of extended 2-error-correcting BCH codes

Since they are quasiperfect the 2-error-correcting BCH codes have covering radius equal to 3. Let \hat{B} be the extension of such a code B . The minimum weight of \hat{B} is 6 and \hat{B} is included in P^2 whose minimum weight is 4. Then there are cosets of \hat{B} of minimum weight 4. Let H be any coset of \hat{B} ; we are interested in the minimum weight of H . It is well-known that the code \hat{B} is invariant under the affine permutation group of G [4, 24]; in particular it is invariant under the translations (i.e. multiplications by X^h). So we can assume that H has at least one minimum weight codeword whose support contains 0. Then if the coset $X^0 + H$ is different from \hat{B} , its minimum weight cannot be greater than the covering radius of B . So it is clear that *the covering radius of any 2-error-correcting extended BCH code equals 4*; equivalently the minimum weight of any H is less than or equal to 4. Another remark comes from the fact that the automorphism group of \hat{B} contains the affine permutations of G : all cosets H of minimum weight 1 (respectively 2) have the same weight distribution.

Notation: In this Section we often will use the weights of the dual \hat{B}^\perp of \hat{B} , given in Tables 1 and 2. They will be denoted as follows

$$\begin{aligned} m \text{ odd} : \quad & \gamma_1 = 2^{m-1} - 2^{(m-1)/2}, \quad \gamma_2 = 2^{m-1}, \quad \gamma_3 = 2^{m-1} + 2^{(m-1)/2}, \\ m \text{ even} : \quad & \delta_1 = 2^{m-1} - 2^{m/2}, \quad \delta_2 = 2^{m-1} - 2^{m/2-1}, \quad \delta_3 = 2^{m-1}, \\ & \delta_4 = 2^{m-1} + 2^{m/2-1}, \quad \delta_5 = 2^{m-1} + 2^{m/2}. \end{aligned} \quad (17)$$

3.1 Cosets $y + \hat{B}$, $y \in P^2 \setminus \hat{B}$

In this section we study the cosets $y + \hat{B}$ with $y \in P^2 \setminus \hat{B}$. Since the covering radius of \hat{B} and the minimum weight of P^2 both equal 4, such cosets have minimum weight 4. By definition of P^2 there is a one-to-one correspondence between these cosets and the syndromes $(0, 0, \phi_3(y))$, (see Definition 3 and Remark 1). Recall that the dimension of P^2 equals $\dim \hat{B} + m$. So there are $2^m - 1$ such cosets - i.e. $\phi_3(y)$ can take any value in G^* . We will denote by C_y the code $\hat{B} \cup (y + \hat{B})$. We want to obtain the weight enumerator of the code C_y^\perp , for any y . We proved in Lemma 2(i) that C_y^\perp is a union of some cosets $x + P^{m-1}$, x in \hat{B}^\perp . In accordance with this result, it is sufficient to determine, for each type ((I) for odd m , (II) and (III) for even m) the number of cosets D of that type which satisfy $yD = \{0\}$. It is very simple to do so when m is odd; the following lemma will allow us to treat the even case.

Lemma 3 Assume that m is even. Let $y \in P^2 \setminus \hat{B}$. Denote by ∇ , the number of cosets of type (III) contained in C_y^\perp . Then the value of ∇ depends on y and there are two distinct cases:

- (i) If $\phi_3(y) = \alpha^{3k}$, $k \in [0, n/3[$, then $\nabla = \nabla_1$ where
 - 1. If $m \equiv 0 \pmod{4}$ then $\nabla_1 = (2^{m-1} - 2^{m/2} - 1)/3$.
 - 2. If $m \not\equiv 0 \pmod{4}$ then $\nabla_1 = (2^{m-1} + 2^{m/2} - 1)/3$.
- (ii) If $\phi_3(y) = \alpha^{3k+r}$, $r \in \{1, 2\}$ and $k \in [0, n/3[$, then $\nabla = \nabla_2$ where
 - 1. If $m \equiv 0 \pmod{4}$ then $\nabla_2 = (2^{m-1} + 2^{m/2-1} - 1)/3$.
 - 2. If $m \not\equiv 0 \pmod{4}$ then $\nabla_2 = (2^{m-1} - 2^{m/2-1} - 1)/3$.

Proof: From Proposition 5, the cosets of type (III) are the $sh_j(\tau) + P^{m-1}$, $j \in [0, n/3[$. Since $yP^{m-1} = \{0\}$, the number of such cosets D satisfying $yD = \{0\}$ equals the number of j such that $ysh_j(\tau) = 0$. Moreover this last equality is equivalent to $\phi_n(ysh_j(\tau)) = 0$, because $\phi_n(ysh_j(\tau))$ equals $(ysh_j(\tau))_0$ (cf. Proposition 2). Applying Proposition 4, we obtain

$$\phi_n(ysh_j(\tau)) = \sum_{i < n} \phi_i(y) \phi_{n-i}(sh_j(\tau)) = \text{Tr}(\phi_3(y) \phi_{n-3}(sh_j(\tau))), \quad (18)$$

since $\phi_s(\tau) = 0$ unless s is in the cyclotomic coset of $n-3$. From Proposition 5 (ii) we have $\phi_{n-3}(sh_j(\tau)) = \alpha^{-3j}$.

(i) Since \hat{B} is invariant under the shift, we can suppose that $\phi_3(y) = 1$. Then formula (18) becomes

$$\phi_n(ysh_j(\tau)) = \text{Tr}(\alpha^{-3j}) \text{ for all } j \in [0, n/3[.$$

Now we use Proposition 2 and (13) in the following equalities:

$$\begin{aligned} \nabla_1 &= \text{card} \{ sh_j(\tau) \mid j \in [0, n/3[, \phi_n(ysh_j(\tau)) = 0 \} \\ &= \text{card} \{ sh_j(\tau) \mid j \in [0, n/3[, \text{Tr}(\alpha^{-3j}) = 0 \} \\ &= \text{card} \{ s \in [0, n/3[\mid M_\tau(\alpha^s) = 0 \} = \frac{(2^m - 1) - \omega(\tau)}{3}. \end{aligned}$$

Indeed $M_\tau(Z) = \text{Tr}(\phi_{n-3}(\tau)Z^3) = \text{Tr}(Z^3)$. From Corollary 1, the weight of τ is equal to $2^{m-1} + 2^{m/2}$ when 4 divides m and is equal to $2^{m-1} - 2^{m/2}$ otherwise.

(ii) We can suppose that $\phi_3(y) = \alpha^r$, $r = 1$ or 2 . Then formula (18) becomes:

$$\phi_n(ysh_j(\tau)) = \text{Tr}(\alpha^{-3j+r}), \text{ for all } j \in [0, n/3[.$$

Recall that $x^{(r)}$, $r = 1$ or 2 , denotes the element of C_β which satisfies $\phi_{n-3}(x^{(r)}) = \alpha^r$ (cf. Proposition 5). Then, as previously, we obtain the following equalities:

$$\begin{aligned} \nabla_2 &= \text{card} \{ sh_j(\tau) \mid j \in [0, n/3[, \phi_n(ysh_j(\tau)) = 0 \} \\ &= \text{card} \{ sh_j(\tau) \mid j \in [0, n/3[, \text{Tr}(\alpha^{-3j+r}) = 0 \} \\ &= \text{card} \{ s \in [0, n/3[\mid M_{x^{(r)}}(\alpha^s) = 0 \} = \frac{(2^m - 1) - \omega(x^{(r)})}{3}. \end{aligned}$$

Indeed $M_{x^{(r)}}(Z) = \text{Tr}(\phi_{n-3}(x^{(r)})Z^3) = \text{Tr}(\alpha^r Z^3)$. The cosets $x^{(r)} + P^{m-1}$ are of type (II) and from Corollary 1, the weight of $x^{(r)}$ is equal to $2^{m-1} - 2^{m/2-1}$ when 4 divides m ; it is equal to $2^{m-1} + 2^{m/2-1}$ otherwise.

□

weights	$m \equiv 0 \pmod{4}$, $\phi_3(y) = \alpha^{3k}$	$m \equiv 0 \pmod{4}$, $\phi_3(y) = \alpha^{3k+r}$
0	1	1
δ_1	$2^{m-2}(2^{m-1} - 2^{m/2} - 1)/3$	$2^{m-2}(2^{m-1} + 2^{m/2-1} - 1)/3$
δ_2	$2^m(2^m + 2^{m/2} - 2)/3$	$2^m(2^m - 2^{m/2-1} - 2)/3$
δ_3	$2^{m-1}(2^{m-1} - 2^{m/2} - 1) + 2^{m+1} - 2$	$2^{m-1}(2^{m-1} + 2^{m/2-1} - 1) + 2^{m+1} - 2$
δ_4	$2^m(2^m + 2^{m/2} - 2)/3$	$2^m(2^m - 2^{m/2-1} - 2)/3$
δ_5	$2^{m-2}(2^{m-1} - 2^{m/2} - 1)/3$	$2^{m-2}(2^{m-1} + 2^{m/2-1} - 1)/3$
2^m	1	1
weights	$m \not\equiv 0 \pmod{4}$, $\phi_3(y) = \alpha^{3k}$	$m \not\equiv 0 \pmod{4}$, $\phi_3(y) = \alpha^{3k+r}$
0	1	1
δ_1	$2^{m-2}(2^{m-1} + 2^{m/2} - 1)/3$	$2^{m-2}(2^{m-1} - 2^{m/2-1} - 1)/3$
δ_2	$2^m(2^m - 2^{m/2} - 2)/3$	$2^m(2^m + 2^{m/2-1} - 2)/3$
δ_3	$2^{m-1}(2^{m-1} + 2^{m/2} - 1) + 2^{m+1} - 2$	$2^{m-1}(2^{m-1} - 2^{m/2-1} - 1) + 2^{m+1} - 2$
δ_4	$2^m(2^m - 2^{m/2} - 2)/3$	$2^m(2^m + 2^{m/2-1} - 2)/3$
δ_5	$2^{m-2}(2^{m-1} + 2^{m/2} - 1)/3$	$2^{m-2}(2^{m-1} - 2^{m/2-1} - 1)/3$
2^m	1	1

Table 3: The two distinct weight distributions of the codes C_y^\perp , $y \in P^2 \setminus \hat{B}$, m even.

Theorem 3 Set $N = 2^m$; let \hat{B} be the 2-error-correcting extended BCH code of length N . Let $y \in P^2 \setminus \hat{B}$ and let C_y be the code $(y + \hat{B}) \cup \hat{B}$.

- (i) If m is odd, all cosets $y + \hat{B}$ have the same weight distribution. It is the polynomial W_4 , given in Table 8. The weight enumerator of C_y^\perp is

$$W_{C_y^\perp}(X, Y) = X^N + (2^{2m-2} - 2^{m-1})X^{N-\gamma_1}Y^{\gamma_1} + (2^{2m-1} + 2^m - 2)X^{N-\gamma_2}Y^{\gamma_2} + (2^{2m-2} - 2^{m-1})X^{N-\gamma_3}Y^{\gamma_3} + Y^N. \quad (19)$$

- (ii) If m is even, there are two distinct weight distributions for the cosets $y + \hat{B}$. They are the polynomials $W_4^{(2)}$ and $W_4^{(3)}$, given in Table 9. These distributions depend on the divisibility of m by 4. They are obtained from the weight enumerators of the codes C_y^\perp we give in Table 3.

Proof: (i) When m is odd, the code \hat{B}^\perp consists of P^{m-1} and of $2^m - 1$ cosets D of type (I). Clearly $yP^{m-1} = \{0\}$. Since the code C_y^\perp is a hyperplane of \hat{B}^\perp , the number of cosets D such that $yD = \{0\}$ equals $2^{m-1} - 1$ and does not depend on y . Thus, with Table 1, we obtain immediately the weight enumerator (19). We deduce the weight distribution of any coset $y + \hat{B}$ by applying formula (5).

(ii) Assume that m is even and set $\nu = n/3$. Then \hat{B}^\perp consists of P^{m-1} , of 2ν cosets of type (II) and of ν cosets of type (III). Let D be any coset of type (III). The weight enumerator of the code C_y^\perp is uniquely determined by the number ∇ of cosets D such that $yD = \{0\}$. This number ∇ is given by Lemma 3: there are two distinct values of ∇ , denoted by ∇_1 and ∇_2 , depending on the value of $\phi_3(y)$. That means that there are two distinct weight distributions for the codes C_y^\perp .

Let $\bar{\nabla}$ be the number of cosets of type (II) contained in C_y^\perp . Since the code C_y^\perp contains P^{m-1} and $2^{m-1} - 1$ other cosets, then $\bar{\nabla}$ is equal to $2^{m-1} - 1 - \nabla$. The number of codewords of a given weight δ_i in a coset is known (cf. Table 2). Let us denote by A_k the number of codewords of C_y^\perp of weight k . We obtain

$$\begin{aligned} A_0 = A_N = 1 & & A_{\delta_1} = 2^{m-2}\nabla & A_{\delta_2} = 2^m\bar{\nabla} \\ A_{\delta_3} = 3 \cdot 2^{m-1}\nabla + (2^{m+1} - 2) & & A_{\delta_4} = A_{\delta_2} & A_{\delta_5} = A_{\delta_1} . \end{aligned}$$

Indeed δ_1, δ_3 and δ_5 are the weights of cosets of type (III), δ_2 and δ_4 are the weights of cosets of type (II). We must add the codewords of P^{m-1} : the null vector, the all-one vector and $2^{m+1} - 2$ codewords of weight δ_3 .

Using Lemma 3 we can give in Table 3 the precise value of A_k , depending on m . We deduce the weight distribution of the cosets $y + \hat{B}$ by applying formula (5): there are two distinct distributions depending respectively on ∇_1 and ∇_2 (which only depend on m).

□

Corollary 2 *Notation is that of Theorem 3; m is even. Recall that any coset $y + \hat{B}$ has minimum weight 4. Let Δ_y be the number of codewords of weight 4 in the coset $y + \hat{B}$. Then*

$$\Delta_y = 2^{m-2}\nabla \quad \text{where } \nabla \text{ is given by Lemma 3.}$$

Proof: We apply formula (4); knowing the weight enumerator of the code C_y^\perp , we want to obtain a coefficient of the weight enumerator of C_y . The parameters are here $v = N = 2^m$ and $j = 2^m - 4$. We have also

$$k - j = \dim(C_y) - j = (2^m - 2m) - (2^m - 4) = 4 - 2m$$

which implies $2^{k-j} = \frac{16}{2^{2m}}$. Now we write the j th moment:

$$\left(\begin{matrix} 2^m \\ 2^m - 4 \end{matrix} \right) + \Delta_y = \frac{16}{2^{2m}} \left(\left(\begin{matrix} 2^m \\ 4 \end{matrix} \right) + \sum_{i=1}^5 \left(\begin{matrix} 2^m - \delta_i \\ 4 \end{matrix} \right) A_{\delta_i} \right) ,$$

yields, using a computer,

$$\begin{aligned} \Delta_y &= - \left(\begin{matrix} 2^m \\ 2^m - 4 \end{matrix} \right) + \frac{16}{2^{2m}} 2^{m-2}\nabla \sum_{i \in \{1,5\}} \left(\begin{matrix} 2^m - \delta_i \\ 4 \end{matrix} \right) \\ &\quad + \frac{16}{2^{2m}} (3 \cdot 2^{m-1}\nabla + (2^{m+1} - 2)) \left(\begin{matrix} 2^m - \delta_3 \\ 4 \end{matrix} \right) + \frac{16}{2^{2m}} 2^m \bar{\nabla} \sum_{i \in \{2,4\}} \left(\begin{matrix} 2^m - \delta_i \\ 4 \end{matrix} \right) \\ &= 2^{m-2}\nabla \end{aligned}$$

(replacing $\bar{\nabla}$ by $2^{m-1} - 1 - \nabla$). Note that the number of codewords of weight 4 in C_y is the same as the number of codewords of weight 4 in the coset $y + \hat{B}$, since the minimum weight of \hat{B} is 6.

□

Remark 3: The result above shows clearly that the two weight distributions we announced in Theorem 3 are distinct. Indeed, in accordance with Lemma 3, it is impossible to have $\nabla_1 = \nabla_2$.

3.2 Cosets $y + \hat{B}$, $y \in P \setminus P^2$

Now we will study the cosets $y + \hat{B}$ y in $P \setminus P^2$; C_y still denotes the code $\hat{B} \cup (y + \hat{B})$. Let $H = y + \hat{B}$. Since the minimum weight of P is 2, there are cosets H of minimum weight 2; such a coset has only one codeword of weight 2. All codewords of weight 2 are in $P \setminus P^2$; then there are $2^{m-1}(2^m - 1)$ cosets H of minimum weight 2. The syndromes of the cosets H are the

$$S(y) = (0, \phi_1(y), \phi_3(y)) \quad \text{where } \phi_1(y) \neq 0, \quad y \in P \setminus P^2.$$

There are $2^m(2^m - 1)$ cosets H and finally there are also $2^{m-1}(2^m - 1)$ cosets H of minimum weight 4.

We want to obtain the weight enumerator of C_y^\perp ; we know from Lemma 2 that C_y^\perp contains exactly one half of the elements of $x + P^{m-1}$, for any $x \in \hat{B}^\perp \setminus P^{m-1}$. Then we must describe, for any x , the set of elements of $x + P^{m-1}$ contained in C_y^\perp - i.e. orthogonal to y . So, for a given y , this set depends on x . However some properties appear which reduce the problem. By applying the following lemma, we will obtain a very simple expression of the weight enumerator of C_y^\perp .

Lemma 4 Let $y \in P \setminus P^2$, $x \in \hat{B}^\perp \setminus P^{m-1}$ and set $D = x + P^{m-1}$. Let λ be a weight of D such that $\lambda \neq 2^{m-1}$ and suppose that $\omega(x) = \lambda$. We denote by D_λ the number of codewords of D of weight λ . Set

$$\tilde{D}_\lambda = \text{card} \{ a \in D \mid \omega(a) = \lambda \text{ and } \langle y, a \rangle = 0 \}.$$

Then $\tilde{D}_\lambda \in \{ 0, \frac{1}{2}D_\lambda, D_\lambda \}$ and $\tilde{D}_\lambda = \tilde{D}_{2^m - \lambda}$. Moreover if there are only two non-zero weights in D - i.e. D is of type (II) and its weights are δ_2 and δ_4 - then we have:

$$\tilde{D}_{\delta_2} = \tilde{D}_{\delta_4} = \frac{1}{2}D_{\delta_2} = \frac{1}{2}D_{\delta_4} = 2^{m-1}.$$

Proof: We denote by U the set $\{ 0, 2^{m-1}, 2^m \}$ which is the set of the weights of P^{m-1} . Since $yx \in P^{m-1}$, we have $\omega(yx) \in U$. The value of $\omega(yx)$ equals the number of $g \in G$ such that $\langle y, X^g x \rangle = 1$ (cf. Proposition 3). Let κ be the dimension of the kernel of the symplectic form associated to D . From Proposition 6, the set of the $X^g x, g \in G$, equals the set of the codewords of D of weight λ ; moreover $X^g x = x$ for 2^κ elements g - i.e. $D_\lambda = 2^{m-\kappa}$. Hence we have:

$$\begin{aligned} \tilde{D}_\lambda &= 2^{-\kappa} \text{card} \{ g \in G \mid \langle y, X^g x \rangle = 0 \} \\ &= 2^{-\kappa} (2^m - \omega(yx)). \end{aligned}$$

Since $\omega(yx) \in U$, we can deduce that \tilde{D}_λ can only take one of the three values: 0, $\frac{1}{2}D_\lambda$ or D_λ .

Since $\omega(y)$ is even then $\langle y, \mathbf{1} \rangle = 0$. That implies that for all $a \in D$, $\langle y, a \rangle$ is equal to $\langle y, a + \mathbf{1} \rangle$ (recall that $\mathbf{1} \in P^{m-1}$). That means that there are in D as much elements of weight λ as of weight $2^m - \lambda$ orthogonal to y . Then $\tilde{D}_\lambda = \tilde{D}_{2^m - \lambda}$.

Assume now that D has only two weights, δ_2 and δ_4 . Since $\delta_2 = 2^m - \delta_4$, we have clearly $\tilde{D}_{\delta_2} = \tilde{D}_{\delta_4}$. One half of the elements of D is orthogonal to y ; thus the property $2^m = \tilde{D}_{\delta_2} + \tilde{D}_{\delta_4}$ completes the proof.

□

Weight	m odd , $d(y) = 2$	m odd , $d(y) = 4$
0	1	1
γ_1	2^{2m-2}	$2^{2m-2} - 2^{m-1}$
γ_2	$2^{2m-1} - 2$	$2^{2m-1} + 2^m - 2$
γ_3	2^{2m-2}	$2^{2m-2} - 2^{m-1}$
2^m	1	1

Weight	m even , $d(y) = 2$	m even , $d(y) = 4$
0	1	1
δ_1	$2^{m-3}(2^m + 2)/3$	$2^{m-3}(2^m - 4)/3$
δ_2	$2^m(2^m - 1)/3$	$2^m(2^m - 1)/3$
δ_3	$2^{2m-2} + 2^{m-1} - 2$	$2^{2m-2} + 2^m - 2$
δ_4	$2^m(2^m - 1)/3$	$2^m(2^m - 1)/3$
δ_5	$2^{m-3}(2^m + 2)/3$	$2^{m-3}(2^m - 4)/3$
2^m	1	1

Table 4: The two distinct weight distributions of the codes C_y^\perp , $y \in P \setminus P^2$; the minimum weight of C_y is denoted by $d(y)$.

Theorem 4 Set $N = 2^m$; let \hat{B} be the 2-error-correcting extended BCH code of length N . Let $y \in P \setminus P^2$; let C_y be the code $(y + \hat{B}) \cup \hat{B}$ and denote by $d(y)$ the minimum weight of the coset $y + \hat{B}$.

There are two distinct weight distributions for the cosets $y + \hat{B}$. The first one corresponds to cosets of minimum weight 2; the second one corresponds to cosets of minimum weight 4. The weight enumerators of the codes C_y^\perp are given in Table 4. When m is odd and $d(y) = 4$, we note that the weight enumerator of C_y^\perp equals the polynomial we obtained previously, when $y \in P^2 \setminus \hat{B}$. (cf. Theorem 3 (i)).

When m is odd, the weight distributions of the cosets are respectively denoted by W_2 and W_4 and given in Table 8. When m is even they are denoted by W_2 and $W_4^{(1)}$ and given in Table 9.

Proof: Notation is that of Lemma 4. In all cases we denote by D any coset $x + P^{m-1}$, $x \in \hat{B}^\perp \setminus P^{m-1}$, and by A_j the number of codewords of weight j in C_y^\perp .

1. Assume that m is odd; so the cosets D are all of type (I). Recall that the three weights of D are the γ_i 's, $i \in [1, 3]$, with $\gamma_2 = 2^{m-1}$ and $\gamma_1 = 2^m - \gamma_3$.

First $A_{\gamma_1} = A_{\gamma_3}$, since $\bar{D}_{\gamma_1} = \bar{D}_{\gamma_3}$, for all D (from Lemma 4). Let us denote A_{γ_1} by I . Since the number of elements of C_y^\perp equals 2^{2m} , A_{γ_2} is easily deduced. We obtain:

$$A_0 = A_N = 1, \quad A_{\gamma_1} = A_{\gamma_3} = I, \quad A_{\gamma_2} = 2^{2m} - A_{\gamma_1} - A_{\gamma_3} - 2 = 2^{2m} - 2I - 2.$$

Now we apply formula (4) with $E = C_y^\perp$, $v = N$, $j = 2^m - 2$ and $k - j = 2 - 2m$; the A'_j 's are the coefficients of the weight enumerator of C_y . Since $A'_0 = 1$ and $A'_1 = 0$ we have

$$\binom{2^m}{2^m - 2} + A'_2 = \frac{4}{2^{2m}} \left(\binom{2^m}{2} + \sum_{i=1}^3 \binom{2^m - \gamma_i}{2} A_{\gamma_i} \right)$$

(where the γ_i 's are given by (17)). Hence

$$\begin{aligned}
A'_2 &= 2^{2-2m} \left(\frac{2^m(2^m-1)}{2} + \frac{(2^{m-1} + 2^{(m-1)/2} - 1)(2^{m-1} + 2^{(m-1)/2})}{2} I \right. \\
&\quad + \frac{(2^{m-1} - 1)2^{m-1}(2^{2m} - 2I - 2)}{2} \\
&\quad \left. + \frac{(2^{m-1} - 2^{(m-1)/2} - 1)(2^{m-1} - 2^{(m-1)/2})}{2} I \right) - 2^{m-1}(2^m - 1) \\
&= 1 - 2^{m-1} + 2^{1-m} J.
\end{aligned}$$

Thus the value of I is uniquely determined by that of A'_2 . If $d(y) = 2$ then $A'_2 = 1$ implies $I = 2^{2m-2}$. If $d(y) = 4$ then $A'_2 = 0$ implies $I = 2^{2m-2} - 2^{m-1}$. Replacing I by its value, we obtain Table 4 (m odd). When $d(y) = 4$ we recognize the polynomial (19). This result was foreseeable because of the combinatorial properties of the code B in the odd case; all its cosets of minimum weight 3 have the same weight distribution. However we show here that these cosets correspond to strongly different objects.

2. Assume that m is even. The code \hat{B}^\perp contains $2(2^m - 1)/3$ cosets D of type (II). These cosets have two weights, δ_2 and δ_4 . It comes immediately from Lemma 4 that \tilde{D}_{δ_2} and \tilde{D}_{δ_4} both equal 2^{m-1} , for all D . Hence for any code C_y^\perp we have:

$$A_{\delta_2} = A_{\delta_4} = 2^m(2^m - 1)/3.$$

Furthermore the code \hat{B}^\perp contains $(2^m - 1)/3$ cosets D of type (III); such cosets have three weights, denoted by δ_1 , δ_3 and δ_5 . These weights are different from δ_2 and δ_4 ; moreover $\delta_3 = 2^{m-1}$ and $\delta_1 = 2^m - \delta_5$. Then we proceed as in 1., when we treat cosets of type (I). We have immediately $A_0 = A_N = 1$ and $A_{\delta_1} = A_{\delta_5}$; we denote A_{δ_1} by I . Now we can deduce A_{δ_3} :

$$A_{\delta_3} = 2^{2m} - 2A_{\delta_1} - 2A_{\delta_2} - 2 = 2^m \left(\frac{2^m + 2}{3} \right) - 2I - 2.$$

Let $j = 2^m - 2$; the j th equality of (4) is:

$$\binom{2^m}{2^m - 2} + A'_2 = \frac{4}{2^{2m}} \left(\binom{2^m}{2} + \sum_{i=1}^5 \binom{2^m - \delta_i}{2} A_{\delta_i} \right)$$

(where δ_i is given by (17)). Solving it we obtain A'_2 :

$$A'_2 = 2^{2-m} I - \frac{2^{m-1} - 2}{3}.$$

If $d(y) = 2$ then $A'_2 = 1$ implies $I = (2^{2m-3} + 2^{m-2})/3$. If $d(y) = 4$ then $A'_2 = 0$ implies $I = (2^{2m-3} - 2^{m-1})/3$. Then we complete Table 4 (m even).

For any m we obtain the expressions of the weight enumerators $W_{y+\hat{B}}(X, Y)$, by means of formula (5).

□

If a coset $y + \hat{B}$ has minimum weight 2, it has only one word of weight 2. If it has minimum weight 4, the number of its minimum weight codewords equals that of the corresponding code C_y . We can determine this number in the same manner as we did in Section 3.1 (see Corollary 2). We present the result in the following corollary; note that Δ_y does not depend on y in this case.

Corollary 3 *Notation is that of Theorem 4. Assume that the coset $y + \hat{B}$ has minimum weight 4 and denote by Δ_y the number of codewords of weight 4 in this coset. Then*

$$\begin{aligned} m \text{ odd} &\implies \Delta_y = 2^{m-2} \left(\frac{2^{m-1} - 1}{3} \right) \\ m \text{ even} &\implies \Delta_y = 2^{m-1} \left(\frac{2^{m-2} - 1}{3} \right) \end{aligned}$$

Remark 4: When $y \in P^2 \setminus \hat{B}$ and m is even, we found other cosets of minimum weight 4. From Corollary 2, we know that the number of minimum weight codewords of these cosets equals $2^{m-2} \nabla$. Note that it is impossible to have

$$2^{m-2} \nabla = 2^{m-1} \left(\frac{2^{m-2} - 1}{3} \right),$$

unless $m = 2$. Hence we have clearly three distinct weight distributions for the cosets of minimum weight 4.

3.3 Cosets $y + \hat{B}$, $y \in \mathcal{A} \setminus P$

In this section we study cosets $y + \hat{B}$ such that y is in $\mathcal{A} \setminus P$; C_y still denotes the code $\hat{B} \cup (y + \hat{B})$. By definition, the radical P of \mathcal{A} contains all codewords of even weight. Hence y has an odd weight; therefore every codeword $y + \hat{B}$ has an odd weight. The syndromes of such cosets are

$$\mathcal{S}(y) = (1, \phi_1(y), \phi_3(y)),$$

where the $\phi_i(y)$, $i \in \{1, 3\}$, take any value in \mathbf{G} . Let H be any coset $y + \hat{B}$; there are 2^{2m} cosets H . Clearly there are cosets H of minimum weight 1. Suppose that $\omega(y) = 1$, which means $y = X^g$, for some g . Then $\phi_i(y) = g^i$. So the syndromes of the cosets of minimum weight 1 are: $(1, g, g^3)$, $g \in \mathbf{G}$. The remaining cosets H have minimum weight 3. Finally there are 2^m cosets of minimum weight 1 and $2^m(2^m - 1)$ cosets of minimum weight 3.

We want to obtain the weight enumerator of any code C_y^\perp , $y \in \mathcal{A} \setminus P$. Let $D = x + P^{m-1}$ be a coset of P^{m-1} contained in \hat{B}^\perp . From Lemma 2, we are in the same situation as in Section 3.2: one half of the elements of D is orthogonal to y . We must determine the number of such elements of a given weight, for every D . As in Section 3.2, we first present some properties which will reduce the problem.

Lemma 5 *Let $y \in \mathcal{A} \setminus P$ and $x \in \hat{B}^\perp$; set $D = x + P^{m-1}$. Let λ be a weight of D . We denote by D_λ the number of codewords of D of weight λ . Set*

$$\tilde{D}_\lambda = \text{card} \{ a \in D \mid \omega(a) = \lambda \text{ and } \langle y, a \rangle = 0 \}.$$

Then $\tilde{D}_\lambda = D_\lambda - \tilde{D}_{2^m - \lambda}$. That means that the code C_y^\perp contains exactly one half of the codewords of \hat{B}^\perp of weight 2^{m-1} .

Suppose now that $\lambda \neq 2^{m-1}$ and $x \notin P^{m-1}$. Let κ be the dimension of the kernel of the symplectic form associated to D . Assuming that y is a minimum weight codeword in C_y , we have :

$$\begin{aligned} \text{if } \omega(y) = 1 & \quad \text{then} \quad \tilde{D}_\lambda = 2^{-\kappa}(2^m - \lambda) \\ \text{if } \omega(y) = 3 & \quad \text{then} \quad \tilde{D}_\lambda \in \{ 2^{-\kappa}\lambda, 2^{-\kappa}(2^m - \lambda) \} . \end{aligned}$$

Proof: 1. We have $\langle y, \mathbf{I} \rangle = 1$, since the weight of y is odd. That means

$$\langle y, a + \mathbf{I} \rangle = \langle y, a \rangle + 1, \text{ for all } a \in D,$$

which implies

$$\tilde{D}_\lambda = \text{card} \{ a \in D \mid \omega(a) = 2^m - \lambda \text{ and } \langle y, a \rangle = 1 \} = D_{2^m - \lambda} - \tilde{D}_{2^m - \lambda}.$$

Moreover the cosets D satisfy $D_\lambda = D_{2^m - \lambda}$. When $\lambda = 2^{m-1}$ the formula above implies $2\tilde{D}_\lambda = D_\lambda$, for any D . Since \hat{B}^\perp is a union of some cosets D we can conclude that one half of the codewords of \hat{B}^\perp of weight 2^{m-1} is contained in C_y^\perp .

2. Note that a coset $y + \hat{B}$ of minimum weight 1 does not contain codewords of weight 3. Suppose now that $\lambda \neq 2^{m-1}$, $x \notin P^{m-1}$ and $\omega(x) = \lambda$. From Proposition 6, we have

$$\{ a \in D \mid \omega(a) = \lambda \} = \{ X^g x \mid g \in G \} \quad \text{and} \quad D_\lambda = 2^{m-\kappa}.$$

Then

$$\tilde{D}_\lambda = \text{card} \{ X^g x \mid g \in G \text{ and } \langle y, X^g x \rangle = 0 \}.$$

Applying Proposition 3, we obtain

$$\tilde{D}_\lambda = \frac{1}{2^\kappa} \text{card} \{ g \in G \mid \langle y, X^g x \rangle = 0 \} = 2^{-\kappa}(2^m - \omega(yx)). \quad (20)$$

If $\omega(y) = 1$ then $\omega(yx) = \omega(x) = \lambda$. We suppose now that $\omega(y) = 3$. We can always rewrite y as follows:

$$\begin{aligned} y &= X^{g_1} + X^{g_2} + X^{g_3} = X^{g_1+g_2+g_3} + (X^{g_1} + X^{g_2} + X^{g_3} + X^{g_1+g_2+g_3}) \\ &= X^{g_1+g_2+g_3} + \bar{y} \quad \text{where } \bar{y} \in P^2 \setminus \hat{B}. \end{aligned} \quad (21)$$

Note that g_1, g_2 and g_3 are three distinct elements of G . Since the support of \bar{y} is an affine subspace of G of dimension 2, \bar{y} is clearly a minimum weight codeword of P^2 (i.e. of the Reed-Muller code of order $m-2$). Moreover $x \in P^{m-2}$ implies $\bar{y}x \in P^m$ involving $\bar{y}x \in \{0, \mathbf{I}\}$. Hence

$$\omega(yx) = \omega(X^{\phi_1(y)}x + \bar{y}x) \in \{ \omega(x), 2^m - \omega(x) \},$$

with $\phi_1(y) = g_1 + g_2 + g_3$. Using (20) we can conclude:

$$\begin{aligned} \bar{y}x = 0 & \implies \tilde{D}_\lambda = 2^{-\kappa}(2^m - \lambda) \\ \bar{y}x = \mathbf{I} & \implies \tilde{D}_\lambda = 2^{-\kappa}\lambda. \end{aligned} \quad (22)$$

Recall that $\bar{y}x = 0$ is equivalent to $\bar{y}D = \{0\}$ (see Lemma 2 (i)).

□

Theorem 5 Set $N = 2^m$. Let \hat{B} be the 2-error-correcting extended BCH code of length N . Let $y \in A \setminus P$ and let C_y be the code $(y + \hat{B}) \cup \hat{B}$.

- (i) If m is odd there are two distinct weight distributions for the cosets $y + \hat{B}$: the weight distribution of the cosets of minimum weight 1 and the weight distribution of the cosets of minimum weight 3. These distributions are given in Table 8 as polynomials W_1 and W_3 . The weight enumerators of the corresponding codes C_y are given in Table 5.
- (ii) When m is even there are three distinct weight distributions for the cosets $y + \hat{B}$. All cosets of minimum weight 1 have the same weight distribution. There are two distinct weight distributions for the cosets whose minimum weight is 3. These three distributions are given in Table 9 as polynomials W_1 , $W_3^{(1)}$ and $W_3^{(2)}$. The weight enumerators of the corresponding codes C_y are given in Tables 6 and 7.

Proof: In all cases, we denote by A_λ the number of codewords of C_y^\perp of weight λ and by $d(y)$ the minimum weight of C_y (ie. of the coset $y + \hat{B}$). Notation is that of Lemma 5 and we use Tables 1 and 2 for the weight distribution of \hat{B}^\perp . The values A_0 , A_N and $A_{2^{m-1}}$ do not depend on y . Obviously $A_0 = 1$ and we obtain immediately $A_{2^{m-1}}$ from Lemma 5:

$$A_{2^{m-1}} = \frac{1}{2} \text{card} \{ a \in \hat{B}^\perp \mid \omega(a) = 2^{m-1} \}.$$

Furthermore y has always an odd weight; then $\langle y, \mathbf{I} \rangle = 1$ which yields $A_N = 0$.

- (i) Assume that m is odd. In this case $A_{2^{m-1}} = 2^{2^{m-1}} + 2^{m-1} - 1$. Suppose now that $\lambda \in \{\gamma_1, \gamma_3\}$. The code \hat{B}^\perp consists of $2^m - 1$ cosets $D = x + P^{m-1}$ of type (I) whose associated symplectic forms have kernel of dimension $\kappa = 1$. We suppose that $\omega(x) = \lambda$ and apply Lemma 5:

- 1. If $d(y) = 1$ then

$$A_\lambda = (2^m - 1)\bar{D}_\lambda = (2^m - 1)\frac{2^m - \lambda}{2}.$$

- 2. If $d(y) = 3$ then $y = \bar{y} + X^\theta$ where \bar{y} is an element of P^2 and $\theta = \phi_1(y)$ (see (21)). We know that $\bar{y}x = 0$ for $2^{m-1} - 1$ cosets D and that $\bar{y}x$ equals \mathbf{I} for the 2^{m-1} remaining cosets D (see part 1 of the proof of Theorem 4). Then from Lemma 5 and (22):

$$A_\lambda = (2^{m-1} - 1)\frac{2^m - \lambda}{2} + 2^{m-1}\frac{\lambda}{2} = 2^{m-1}(2^{m-1} - 1) + \lambda/2.$$

Replacing λ by its value, we complete Table 5.

- (ii) Suppose that m is even. Thus $A_{2^{m-1}} = 2^{2^{m-2}} + 3 \cdot 2^{m-2} - 1$. From now on λ is in $\{\delta_1, \delta_2, \delta_4, \delta_5\}$. The code \hat{B}^\perp consists of $2(2^m - 1)/3$ cosets D of type (II) and of $(2^m - 1)/3$ cosets of type (III) which contain all codewords of weight λ . The dimension κ of the kernel of associated symplectic forms is here:

$$\begin{aligned} \text{cosets of type (II)} &\Rightarrow \kappa = 0, \quad \lambda \in \{\delta_2, \delta_4\} \\ \text{cosets of type (III)} &\Rightarrow \kappa = 2, \quad \lambda \in \{\delta_1, \delta_5\}. \end{aligned}$$

We apply Lemma 5:

Weight	$d(y) = 1$	$d(y) = 3$
0	1	1
γ_1	$(2^m - 1)(2^{m-2} + 2^{(m-3)/2})$	$2^{2m-2} - 2^{m-2} - 2^{(m-3)/2}$
γ_2	$2^{2m-1} + 2^{m-1} - 1$	$2^{2m-1} + 2^{m-1} - 1$
γ_3	$(2^m - 1)(2^{m-2} - 2^{(m-3)/2})$	$2^{2m-2} - 2^{m-2} + 2^{(m-3)/2}$

Table 5: The two distinct weight distributions of C_y^\perp , m odd and $y \in \mathcal{A} \setminus P$; $d(y)$ is the minimum weight of the coset $y + \hat{B}$.

Weight	number of words
0	1
δ_1	$((2^m - 1)/3)(2^{m-3} + 2^{m/2-2})$
δ_2	$((2^m - 1)/3)(2^m + 2^{m/2})$
δ_3	$2^{2m-2} + 3 \cdot 2^{m-2} - 1$
δ_4	$((2^m - 1)/3)(2^m - 2^{m/2})$
δ_5	$((2^m - 1)/3)(2^{m-3} - 2^{m/2-2})$

Table 6: The weight distribution of C_y^\perp when m is even, $y \in \mathcal{A} \setminus P^2$ and the minimum weight of the coset $y + \hat{B}$ is 1.

Weight	$m \equiv 0 \pmod{4}$, $\phi_3(\bar{y}) = \alpha^{3k}$	$m \equiv 0 \pmod{4}$, $\phi_3(\bar{y}) = \alpha^{3k+r}$
0	1	1
δ_1	$(2^{2m-3} - 5 \cdot 2^{m-3} - 2^{m/2-2})/3$	$(2^{2m-3} + 2^{m-3} - 2^{m/2-2})/3$
δ_2	$(2^{2m} - 2^{m/2})/3$	$(2^{2m} - 2^{m/2})/3 - 2^{m-1}$
δ_3	$2^{2m-2} + 3 \cdot 2^{m-2} - 1$	$2^{2m-2} + 3 \cdot 2^{m-2} - 1$
δ_4	$(2^{2m} - 2^{m+1} + 2^{m/2})/3$	$(2^{2m} - 2^{m-1} + 2^{m/2})/3$
δ_5	$(2^{2m-3} + 2^{m/2-2})/3 + 2^{m-3}$	$(2^{2m-3} + 2^{m/2-2})/3 - 2^{m-3}$
Weight	$m \not\equiv 0 \pmod{4}$, $\phi_3(\bar{y}) = \alpha^{3k}$	$m \not\equiv 0 \pmod{4}$, $\phi_3(\bar{y}) = \alpha^{3k+r}$
0	1	1
δ_1	$(2^{2m-3} - 2^{m/2-2})/3 + 2^{m-3}$	$(2^{2m-3} - 2^{m/2-2})/3 - 2^{m-3}$
δ_2	$(2^{2m} - 2^{m+1} - 2^{m/2})/3$	$(2^{2m} - 2^{m-1} - 2^{m/2})/3$
δ_3	$2^{2m-2} + 3 \cdot 2^{m-2} - 1$	$2^{2m-2} + 3 \cdot 2^{m-2} - 1$
δ_4	$(2^{2m} + 2^{m/2})/3$	$(2^{2m} + 2^{m/2})/3 - 2^{m-1}$
δ_5	$(2^{2m-3} - 5 \cdot 2^{m-3} + 2^{m/2-2})/3$	$(2^{2m-3} + 2^{m-3} + 2^{m/2-2})/3$

Table 7: The two distinct weight distributions of the codes C_y^\perp , m even, $y \in \mathcal{A} \setminus \hat{B}$, when the minimum weight of the coset $y + \hat{B}$ is 3. These distributions depend on the value of m (4 divides m or not).

1. If $d(y) = 1$ then

$$\lambda \in \{\delta_2, \delta_4\} \Rightarrow A_\lambda = \frac{2(2^m - 1)}{3} \tilde{D}_\lambda = \frac{2(2^m - 1)}{3} (2^m - \lambda)$$

$$\lambda \in \{\delta_1, \delta_5\} \Rightarrow A_\lambda = \frac{2^m - 1}{3} \tilde{D}_\lambda = \frac{2^m - 1}{12} (2^m - \lambda).$$

2. When $d(y) = 3$, we get as in (i): $y = \bar{y} + X^\theta$. We proved in Section 3.1 that there are ∇ cosets D of type (III) (respectively $\bar{\nabla}$ cosets of type (II)) satisfying $\bar{y}D = \{0\}$ (see part 2 of the proof of Theorem 4). Hence we obtain from Lemma 5 and (22):

$$\lambda \in \{\delta_2, \delta_4\} \Rightarrow A_\lambda = \bar{\nabla}(2^m - \lambda) + \left(\frac{2(2^m - 1)}{3} - \bar{\nabla}\right)\lambda$$

$$\lambda \in \{\delta_1, \delta_5\} \Rightarrow A_\lambda = \nabla \frac{2^m - \lambda}{4} + \left(\frac{2^m - 1}{3} - \nabla\right) \frac{\lambda}{4}$$

where the values of ∇ are given by Lemma 3 and $\bar{\nabla} = 2^{m-1} - 1 - \nabla$. There are two distinct values for ∇ depending on the values of $\phi_3(y)$. Thus we obtain two distinct weight distributions for the codes C_y^\perp , replacing λ and ∇ by their values.

In all cases, m odd or even, the polynomials $W_{y+\hat{B}}(X, Y)$ given in Tables 8 and 9 are obtained by applying formula (5).

□

Corollary 4 *Notation is that of Theorem 5. When $d(y) = 1$ the coset $y + \hat{B}$ has only one codeword of weight 1. Suppose that $d(y) = 3$ and let Δ_y be the number of codewords of weight 3 in the coset $y + \hat{B}$. Then*

$$\begin{aligned} m \text{ odd} &\Rightarrow \Delta_y = \frac{2^{m-1} - 1}{3} \\ m \text{ even} &\Rightarrow \Delta_y = \nabla. \end{aligned}$$

Proof: We proceed as in the proof of Corollary 2. We solve here the $(2^m - 3)$ th moment of the weight distribution of C_y^\perp ; we obtain A'_3 which is in fact Δ_y . Note that Δ_y depends on y only when m is even.

□

3.4 Conclusion

Theorem 6 *Let \hat{B} be the binary extended 2-error-correcting BCH code of length 2^m .*

1. *When m is odd there are five distinct weight distributions for the cosets of \hat{B} . Except for the code \hat{B} itself their minimum weights are respectively 1, 2, 3 and 4.*
2. *When m is even there are eight distinct weight distributions for the cosets of \hat{B} . Except for the code \hat{B} itself their minimum weights are respectively 1, 2, two times 3 and three times 4.*

W_i	y in	$d(y)$	A_{γ_1}	A_{γ_2}	A_{γ_3}	A_N
W_1	$\mathcal{A} \setminus P$	1	$2^{(m-1)/2}(2^m - 1)$	0	$-2^{(m-1)/2}(2^m - 1)$	-1
W_2	$P \setminus P^2$	2	2^{m-1}	$-(2^m + 2)$	2^{m-1}	1
W_3	$\mathcal{A} \setminus P$	3	$-2^{(m-1)/2}$	0	$2^{(m-1)/2}$	-1
W_4	$P \setminus P^2$ or $P^2 \setminus \hat{B}$	4	-2^{m-1}	$(2^m - 2)$	-2^{m-1}	1

Table 8: The four distinct weight distributions of cosets of the 2-error-correcting extended BCH codes of length 2^m , m odd. See explanations in Section 3.4.

Proof: The theorem summarizes the results previously stated in Theorems 3, 4 and 5. Remarks 3 and 4 complete the proof.

□

Remark 5: We recalled in the introduction that when m is odd the code B is completely regular. Note that the same property holds for its extension \hat{B} . Indeed each coset of \hat{B} is such that its weight distribution only depends on its minimum weight. We are not surprised by this result which was proved in a more general context in [6, p. 258].

The weight distributions of the cosets $y + \hat{B}$, $y \notin \hat{B}$, are given in Table 8 when m is odd and in Table 9 when m is even. In these tables each row is related with each set of cosets having the same weight distribution. Each weight distribution was calculated with formula (5) in which the polynomials $W_{C_y^\perp}$ and $W_{\hat{B}^\perp}$ are expressed with the weight enumerators of the codes \hat{B}^\perp and C_y^\perp (for the related y). The minimum weight of the cosets is denoted by $d(y)$. The length of the codes is $N = 2^m$. The weight enumerator of the code \hat{B} itself is omitted (since it was given in Tables 1 and 2).

Table 8 The set of weights of \hat{B}^\perp and of the codes C_y^\perp is $\{0, N, \gamma_1, \gamma_2, \gamma_3\}$ (see the values of these weights in (17)). The table gives the coefficients A_j (where j is a weight of \hat{B}^\perp) which appear in the following formula:

$$W_i(X, Y) = \frac{1}{2^{2m+1}} \left((X + Y)^N + \sum_{i=1}^3 A_{\gamma_i} (X + Y)^{N-\gamma_i} (X - Y)^{\gamma_i} + A_N (X - Y)^N \right).$$

There are four distinct weight enumerators $W_{y+\hat{B}}(X, Y)$, $y \notin \hat{B}$. They are denoted by $W_i(X, Y)$, where i is the minimum weight of the coset $y + \hat{B}$.

Table 9 The weights of \hat{B}^\perp and of the codes C_y^\perp are 0, N and δ_i , $i \in [1, 5]$ (see the values of these weights in (17)). The table gives the coefficients A_j (where j is a weight of \hat{B}^\perp) which appear in the following formula:

$$W_{y+\hat{B}}(X, Y) = \frac{1}{2^{2m+1}} \left((X + Y)^N + \sum_{i=1}^5 A_{\delta_i} (X + Y)^{N-\delta_i} (X - Y)^{\delta_i} + A_N (X - Y)^N \right),$$

W_i	y in	$d(y)$	$\phi_3(y)$	A_{δ_1}	A_{δ_2}
W_1	$\mathcal{A} \setminus P$	1		$2^{m/2-1}(2^m - 1)/3$	$2^{m/2+1}(2^m - 1)/3$
W_2	$P \setminus P^2$	2		2^{m-2}	0
$W_3^{(1)}$	$\mathcal{A} \setminus P$	3	$(\phi_1(y))^3 + \alpha^{3k}$	$2^{m/2}(-2^m + 6\nabla_1 + 1)/6$	$2^{m/2}(2^m - 6\nabla_1 - 4)/3$
$W_3^{(2)}$	$\mathcal{A} \setminus P$	3	$(\phi_1(y))^3 + \alpha^{3k+r}$	$2^{m/2}(-2^m + 6\nabla_2 + 1)/6$	$2^{m/2}(2^m - 6\nabla_2 - 4)/3$
$W_4^{(1)}$	$P \setminus P^2$	4		-2^{m-2}	0
$W_4^{(2)}$	$P^2 \setminus \hat{B}$	4	α^{3k}	$2^m(-2^m + 6\nabla_1 + 1)/12$	$2^m(2^m - 6\nabla_1 - 4)/3$
$W_4^{(3)}$	$P^2 \setminus \hat{B}$	4	α^{3k+r}	$2^m(-2^m + 6\nabla_2 + 1)/12$	$2^m(2^m - 6\nabla_2 - 4)/3$

A_{δ_3}	A_{δ_4}	A_{δ_5}	A_N
0	$-2^{m/2+1}(2^m - 1)/3$	$-2^{m/2-1}(2^m - 1)/3$	-1
$-(2^{m-1} + 2)$	0	2^{m-2}	1
0	$-2^{m/2}(2^m - 6\nabla_1 - 4)/3$	$-2^{m/2}(-2^m + 6\nabla_1 + 1)/6$	-1
0	$-2^{m/2}(2^m - 6\nabla_2 - 4)/3$	$-2^{m/2}(-2^m + 6\nabla_2 + 1)/6$	-1
$2^{m-1} - 2$	0	-2^{m-2}	1
$-2^{2m-1} + 3\nabla_1 2^m + 5 \cdot 2^{m-1} - 2$	$2^m(2^m - 6\nabla_1 - 4)/3$	$2^m(-2^m + 6\nabla_1 + 1)/12$	1
$-2^{2m-1} + 3\nabla_2 2^m + 5 \cdot 2^{m-1} - 2$	$2^m(2^m - 6\nabla_2 - 4)/3$	$2^m(-2^m + 6\nabla_2 + 1)/12$	1

Table 9: The seven distinct weight distributions of cosets of the 2-error-correcting extended BCH codes of length 2^m , m even – see explanations in Section 3.4.

where $y \notin \hat{B}$. The ∇_i are given by Lemma 3. The value of ∇ depends on the corresponding value of $\phi_3(y)$ which is also given in the table. When $d(y) = 3$, y and \bar{y} are defined by (21). Recall that α is a primitive root of $GF(2^m)$.

There are seven distinct weight enumerators $W_{y+\hat{B}}(X, Y)$. In the table, they are denoted by W_i when they are weight enumerators of cosets of minimum weight i , $i \in [1, 2]$. When there are l weight enumerators for cosets of minimum weight i , they are denoted by $W_i^{(t)}$, $t \in [1, l]$.

4 Weight distributions of cosets of 2-error-correcting BCH codes

Recall that the 2-error-correcting BCH code of length $n = 2^m - 1$ is denoted by B . In the previous section we gave the weight distributions of the cosets of the extended code B (i.e. of the code \hat{B}). In this section we will state the relations which permit to calculate the weight distributions of the cosets of B by means of those of \hat{B} . At the end we will be able to prove the conjecture of CAMION, COURTEAU and MONTPETIT on the number of distinct weight distributions of the cosets of B , when m is even [9].

Let H be any coset of \hat{B} . If H is a subset of P (respectively of $\mathcal{A} \setminus P$) then every element of H has an even (respectively an odd) weight. We will say that H is an *even weight coset* (respectively an *odd weight coset*). Set $\mathcal{R} = \mathbb{K}^n$ (where $\mathbb{K} = GF(2)$). Each codeword y^* of \mathcal{R} is extended to a codeword y of P , by definition of the extension (see Section 2.1). This correspondence is one-to-one. We will write $y^* = \sum_{g \in G} y_g X^g$

and $y = \sum_{g \in G} y_g X^g$ - where $G^* = G \setminus \{0\}$ and $y_0 = \sum_{g \in G} y_g$. We then define the syndrome of y^* as

$$S(y^*) = (\phi_1(y^*), \phi_3(y^*)). \quad (23)$$

Clearly $\phi_i(y^*) = \phi_i(y)$, for $i > 0$. There are 2^{2m} cosets for the code B .

Lemma 6 *Let H be any even weight coset of \hat{B} and let $(0, \lambda, \mu)$ its syndrome. Then there is exactly one odd weight coset H' whose syndrome is $(1, \lambda, \mu)$ and exactly one coset H^* of B whose syndrome is (λ, μ) . We express as follows the weight enumerators of H , H' and H^* respectively :*

$$V(Z) = \sum_{i=0}^N A_i Z^i, \quad V'(Z) = \sum_{i=0}^N A'_i Z^i, \quad V^*(Z) = \sum_{i=0}^n A_i^* Z^i. \quad (24)$$

where the coefficient of Z^i is the number of codewords of weight i . Then $V^*(Z)$ is uniquely determined from $V(Z)$ and $V'(Z)$ by means of the formulae:

$$\begin{aligned} k \in [1, (N-2)/2] : A_{2k}^* &= A_{2k} - A_{2k-1}^* \\ k \in [0, (N-2)/2] : A_{2k+1}^* &= A'_{2k+1} - A_{2k}^* \end{aligned} \quad (25)$$

and $A_0^* = A_0$.

Proof: Since the extension is a linear mapping there is a one-to-one correspondence between a coset $H^* = y^* + B$ and its extension as an even weight coset $H = y + \hat{B}$, where y is the extended codeword y^* . According to (11) and (23) we have immediately the equalities between the respective syndromes. Now set $H' = X^0 + H$; H' is an odd weight coset whose syndrome equals $(1, \phi_1(y), \phi_3(y))$. We will say that the subset of G corresponding to the non-zero symbols of any codeword x is the *support* of x . To extend an odd weight codeword of \mathcal{R} consists in adding 0 in its support. A codeword with even weight is extended to a codeword of same weight. Thus the first formula of (25) is obvious, since writing

$$V^*(Z) = A_0^* + \sum_{k=1}^{(N-2)/2} (A_{2k-1}^* Z^{2k-1} + A_{2k}^* Z^{2k}) + A_n^*,$$

we obtain immediately the coefficients of $V(Z)$ from those of $V^*(Z)$: $A_0 = A_0^*$, $A_N = A_n^*$ and $A_{2k} = A_{2k-1}^* + A_{2k}^*$. Moreover, since $H' = X^0 + H$, we have for every $k \in [1, (N-2)/2]$:

$$\begin{aligned} A'_{2k+1} &= \text{card} \{ X^0 + c \mid c \in H, \omega(X^0 + c) = 2k+1 \} \\ &= \text{card} \{ c \in H \mid \omega(c) = 2k \text{ and } 0 \notin \text{supp}(c) \} \\ &\quad + \text{card} \{ c \in H \mid \omega(c) = 2k+2 \text{ and } 0 \in \text{supp}(c) \} \\ &= \text{card} \{ c^* \in H^* \mid \omega(c^*) = 2k \} \\ &\quad + \text{card} \{ c^* \in H^* \mid \omega(c^*) = 2k+1 \} \\ &= A_{2k}^* + A_{2k+1}^*, \end{aligned}$$

completing the proof.

□

Theorem 7 Let B be the binary 2-error-correcting BCH code of length $2^m - 1$.

1. When m is odd there are four distinct weight distributions for the cosets of B . Except for the code B itself, their minimum weights are respectively 1, 2 and 3.
2. When m is even there are eight distinct weight distributions for the cosets of B . Except for the code B itself, their minimum weights are respectively 1, two times 2 and four times 3.

Proof: Notations is that of Lemma 6. Let H^* be any coset of B , H the extension of H^* and $H' = X^0 + H$. We denote by $d(H^*)$, $d(H)$ and $d(H')$ the minimum weight of H^* , H and H' . If $d(H^*) = \lambda$ then $d(H) = \lambda$ or $\lambda + 1$ depending on whether λ is even or not. Furthermore $d(H') = \lambda + 1$ or λ depending on whether λ is even or not. Since few cases must be examined it is easy to determine from H^* and $d(H^*)$ the possible H and H' .

1. Assume m is odd. The result is well-known [27]; so we only give the procedure for the effective computation of cosets enumerators. Weight distributions of the cosets of \hat{B} are given in Table 8 as polynomials W_i . In order to obtain the polynomial V^* we indicate the corresponding polynomials V' and V we need for the use of formulae (25).

$d(H^*)$	V	V'
1	W_2	W_1
2	W_2	W_3
3	W_4	W_3

2. From now on m is even. Weight distributions of the cosets of \hat{B} are given in Table 9 as polynomials W_i or $W_i^{(t)}$. The possible weight distributions V^* , by means of V' and V are below summarized.

$d(H^*)$	V	V'
1	W_2	W_1
2	W_2	$W_3^{(1)}$
2	W_2	$W_3^{(2)}$

$d(H^*)$	V	V'
3	$W_4^{(1)}$	$W_3^{(1)}$
3	$W_4^{(1)}$	$W_3^{(2)}$
3	$W_4^{(2)}$	$W_3^{(1)}$
3	$W_4^{(3)}$	$W_3^{(2)}$

We will now explain these results and prove that the eight weight distributions are distinct. All cosets H^* of minimum weight 1 have the same weight distribution; only W_2 (respectively W_1) corresponds to even (respectively odd) weight cosets of minimum weight 2 (respectively 1). It is more complicated when H^* has minimum weight 2 or 3.

For the following it is necessary to recall that a codeword \bar{y} of weight 4 in $P^2 \setminus \hat{B}$ has as its support an affine subspace of dimension 2 of G . A subspace of dimension 2 of G and its cosets are supports of codewords of a same coset of \hat{B} and then correspond to the same syndrome, because \hat{B} contains the RM-code of order $m - 3$ (i.e. the code P^3). These syndromes are the triples $(0, 0, \mu)$, $\mu \in G^*$. Now Let H' be an odd weight coset of \hat{B} of minimum weight 3. Let $y \in H'$ such that $\omega(y) = 3$. According to (21) we have: $y = \bar{y} + X^\theta$ where \bar{y} is an element of P^2 of weight 4 and $\theta = \phi_1(y)$. Thus $\phi_3(y)$ equals $\phi_3(\bar{y}) + \theta^3$.

Suppose that $d(H^*) = 2$. Thus $d(H) = 2$ and $d(H') = 3$. Hence V is the polynomial W_2 . With the notation above the weight distribution of H' is either $W_3^{(1)}$ or $W_3^{(2)}$ depending on whether $\phi_3(\bar{y})$ is or is not a cube (see Table 9). Since $d(H) = 2$ there exists only one codeword of weight 2 in H , let $X^g + X^h$. Thus there is only one codeword y in H' such that $\omega(y) = 3$ and $0 \in \text{supp}(y)$; it is $y = X^0 + X^g + X^h$. Hence

$$\text{supp}(\bar{y}) = \{ 0, g, h, g + h \}, \quad g \neq h \neq 0. \quad (26)$$

Conversely every codeword $X^g + X^h$, with $g \neq h \neq 0$, uniquely determines an H and its corresponding H^* . In accordance with the reminder above, that means that $\phi_3(\bar{y})$ can have any value μ in G^* . Hence both equalities, $V' = W_3^{(1)}$ or $V' = W_3^{(2)}$, occur. From Corollary 4 we know that the coefficient A'_3 of V' equals ∇ . Applying (25) we obtain $A_3^* = A'_3 - A_2^* = \nabla - 1$, which indicates that the two weight distributions are distinct (as are distinct the two possible values of ∇).

From now on $d(H^*) = 3$. Thus $d(H) = 4$ and $d(H') = 3$. Note that a codeword y of H' of weight 3 cannot have 0 in its support. Then we have here

$$y = X^{g_1} + X^{g_2} + X^{g_3} \quad \text{and} \quad \text{supp}(\bar{y}) = \left\{ g_1, g_2, g_3, \sum_{i=1}^3 g_i \right\},$$

where the g_i 's are any nonzero distinct elements of G .

If $\sum_{i=1}^3 g_i = 0$ then $H \subset P^2$, in which case the syndrome of H is any syndrome $(0, 0, \mu)$, $\mu \in G^*$. Moreover $\phi_3(\bar{y}) = \phi_3(y)$. Thus either $V = W_4^{(2)}$ and $V' = W_3^{(1)}$ (μ is a cube) or $V = W_4^{(3)}$ and $V' = W_3^{(2)}$. Assume that $\sum_{i=1}^3 g_i \neq 0$; so $V = W_4^{(1)}$ and the support of \bar{y} is any coset of any subspace of dimension 2 of G . Then V' can be either $W_3^{(1)}$ or $W_3^{(2)}$ and both equalities occur.

In all cases we obtain $A_3^* = A'_3 - A_2^* = \nabla$. According to Corollaries 3 and 2 we know A_4 which, from (25), is equal to $A_4^* + A_3^*$. Thus

$$\begin{aligned} V = W_4^{(1)} &\implies A_4^* = 2^{m-1} \left(\frac{2^{m-2} - 1}{3} \right) - \nabla \\ V = W_4^{(2)} \text{ or } W_4^{(3)} &\implies A_4^* = \nabla(2^{m-2} - 1). \end{aligned}$$

For a same value of ∇ (∇_1 or ∇_2 , see Lemma 3) the two values above are distinct; indeed the equality $\nabla = 2(2^{m-2} - 1)/3$ is impossible unless $m = 2$. That means that the four weight distributions corresponding to $d(H^*) = 3$ are distinct.

□

5 Distance matrices of 2-error-correcting BCH codes

We will denote by B the distance matrix of the code B and by \hat{B} the distance matrix of the code \hat{B} . These matrices, which uniquely determine the weight distributions of cosets, will have u rows and $t + 1$ columns, u being the number of distinct weight distributions of cosets and t the external distance of the code [18]. Each row of the

distance matrix corresponds in fact to each coset weight distribution. Since we determined all weight distributions of cosets of codes B and \hat{B} in previous sections, we are now able to express coefficients of B and of \hat{B} essentially by means of identities (4) with respect to the appropriate code C_y . Recall that the covering radius of B and of \hat{B} equals respectively 3 and 4.

When m is odd, it is well-known that the code B is uniformly packed with parameters $\lambda = (2^{m-1} - 4)/3$ and $\mu = (2^{m-1} - 1)/3$. So the distance matrix of B is the 4×4 following matrix [2][27]:

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \lambda \\ 0 & 0 & 0 & \mu \end{bmatrix}$$

Extending B we obtain the code \hat{B} whose external distance t equals 4. As well as B , the code \hat{B} is completely regular and its covering radius equals its external distance. This last property implies that \hat{B} is a uniformly packed code in the sense of [3] while it does not satisfy the condition $t = e + 1$ (the necessary and sufficient condition for an e -error-correcting code to be uniformly packed, in the usual sense).

Corollary 5 *The distance matrix of the extended 2-error-correcting BCH code of length 2^m , m odd, is the 5×5 following matrix:*

$$\hat{B} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \nu_1 \\ 0 & 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & 0 & \nu_2 \end{bmatrix}$$

where $\mu = (2^{m-1} - 1)/3$, $\nu_1 = (2^{m-2} - 2)\mu$ et $\nu_2 = 2^{m-2}\mu$.

Proof: The values of ν_2 and μ are respectively given by Corollaries 3 and 4. We obtain ν_1 by solving the $(2^m - 4)$ th identity of (4), applied to the code C_y , whose dual weight distribution is given in Table 4. Since \hat{B} has minimum weight 6, the number of codewords of weight 4 in C_y equals the number of codewords of weight 4 in the coset $y + \hat{B}$.

□

From now on we treat the even case. The external distances of codes B and \hat{B} are respectively equal to 5 and 6.

Corollary 6 *Set $N = 2^m$, m even.*

(i) *The distance matrix \hat{B} of the extended 2-error-correcting BCH code of length N is the 8×7 following matrix:*

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{720}N(N-1)(N-4)^2 \\ 0 & 1 & 0 & 0 & 0 & \frac{1}{120}(N-1)(N-4)^2 & 0 & 0 \\ 0 & 0 & 1 & 0 & \frac{1}{24}(N-4)^2 & 0 & \frac{1}{720}(N-4)(N^3 - 11N^2 + 42N - 92) & 0 \\ 0 & 0 & 0 & \nabla_1 & 0 & \frac{1}{120}(N-4)(N^2 - N - 30\nabla_1) & 0 & 0 \\ 0 & 0 & 0 & \nabla_2 & 0 & \frac{1}{120}(N-4)(N^2 - N - 30\nabla_2) & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{24}N(N-4) & 0 & \frac{1}{720}N(N-4)(N^2 - 11N + 40) & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{4}N\nabla_1 & 0 & \frac{1}{720}N(N-4)(N^2 - N - 60\nabla_1) & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{4}N\nabla_2 & 0 & \frac{1}{720}N(N-4)(N^2 - N - 60\nabla_2) & 0 \end{bmatrix}$$

(ii) The distance matrix \mathcal{B} of the 2-error-correcting BCH code of length $N - 1$ is the 8×6 following matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \frac{1}{120}(N-1)(N-4)^2 \\ 0 & 1 & 0 & 0 & \frac{1}{24}(N-4)^2 & \frac{1}{120}(N-6)(N-4)^2 \\ 0 & 0 & 1 & \nabla_1 - 1 & \frac{1}{24}(N-4)^2 - \nabla_1 + 1 & \frac{1}{120}(N-4)(N^2 - 6N - 30\nabla_1 + 20) + \nabla_1 - 1 \\ 0 & 0 & 1 & \nabla_2 - 1 & \frac{1}{24}(N-4)^2 - \nabla_2 + 1 & \frac{1}{120}(N-4)(N^2 - 6N - 30\nabla_2 + 20) + \nabla_2 - 1 \\ 0 & 0 & 0 & \nabla_1 & \frac{1}{24}N(N-4) - \nabla_1 & \frac{1}{120}(N-4)(N^2 - 6N - 30\nabla_1) + \nabla_1 \\ 0 & 0 & 0 & \nabla_2 & \frac{1}{24}N(N-4) - \nabla_2 & \frac{1}{120}(N-4)(N^2 - 6N - 30\nabla_2) + \nabla_2 \\ 0 & 0 & 0 & \nabla_1 & \frac{1}{4}\nabla_1(N-4) & \frac{1}{120}(N-4)(N^2 - N - 60\nabla_1) \\ 0 & 0 & 0 & \nabla_2 & \frac{1}{4}\nabla_2(N-4) & \frac{1}{120}(N-4)(N^2 - N - 60\nabla_2) \end{bmatrix}$$

where the values ∇_1 or ∇_2 of ∇ are given by Lemma 3.

Proof: (i) Table 9 involves the form of \mathcal{B} below. By using results of Section 4, we can express the matrix \mathcal{B} depending of \mathcal{B} :

$$\hat{\mathcal{B}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \Delta \\ 0 & 1 & 0 & 0 & 0 & \lambda & 0 \\ 0 & 0 & 1 & 0 & \mu_1 & 0 & \mu_2 \\ 0 & 0 & 0 & \rho_1 & 0 & \nu_1 & 0 \\ 0 & 0 & 0 & \rho_2 & 0 & \nu_2 & 0 \\ 0 & 0 & 0 & 0 & \epsilon_1 & 0 & \tau_1 \\ 0 & 0 & 0 & 0 & \epsilon_2 & 0 & \tau_2 \\ 0 & 0 & 0 & 0 & \epsilon_3 & 0 & \tau_3 \end{bmatrix} \quad \mathcal{B} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \lambda \\ 0 & 1 & 0 & 0 & \mu_1 & \lambda - \mu_1 \\ 0 & 0 & 1 & \rho_1 - 1 & \mu_1 - \rho_1 + 1 & \nu_1 - \mu_1 + \rho_1 - 1 \\ 0 & 0 & 1 & \rho_2 - 1 & \mu_1 - \rho_2 + 1 & \nu_2 - \mu_1 + \rho_2 - 1 \\ 0 & 0 & 0 & \rho_1 & \epsilon_1 - \rho_1 & \nu_1 - \epsilon_1 + \rho_1 \\ 0 & 0 & 0 & \rho_2 & \epsilon_1 - \rho_2 & \nu_2 - \epsilon_1 + \rho_2 \\ 0 & 0 & 0 & \rho_1 & \epsilon_2 - \rho_1 & \nu_1 - \epsilon_2 + \rho_1 \\ 0 & 0 & 0 & \rho_2 & \epsilon_3 - \rho_2 & \nu_2 - \epsilon_3 + \rho_2 \end{bmatrix}$$

Corollaries 2, 3 and 4 provide respectively the values of ϵ_2 and ϵ_3 , ϵ_1 , ρ_1 and ρ_2 . For the remaining coefficients of $\hat{\mathcal{B}}$, we use formulae (4) with respect to codes C_y , whose dual weight distributions are given in Tables 3, 4, 6 and 7. We must first compute the number Δ of codewords of weight 6 in \hat{B} . Indeed we have not the same situation as in the odd case, because we need the number of codewords of weight 6 in a coset $y + \hat{B}$; this number equals the number of codewords of weight 6 in the corresponding code C_y minus Δ .

□

6 Conclusion

In this paper we treat the problem of weight distributions of cosets of the 2-error-correcting BCH codes. It is clear for us that it is possible to treat other codes by means of the tools we use here. This is quite evident for the codes whose dual weight distributions are given in [23, p. 450 and 453]. The extensions of these codes have duals which are special subcodes of the RM-code of order 2, with dimensions less than or equal to the dimension of the duals of 2-error-correcting extended BCH-codes. Moreover these duals can be described in the same way as we describe the codes \hat{B}^\perp (cf. Section 2.5). Furthermore, some properties we have presented can be placed in a more general context, to give information on weight distributions of cosets of other codes [16].

Acknowledgements

The author would like to thank P. CAMION, B. COURTEAU and A. MONTPETIT who, first of all, suggested the topic and then provided many useful discussions of the general problem of finding weight distributions of cosets of codes. The author was given access to all their numerical results which was extremely helpful in testing conjectures. She is very grateful to C. CARLET for his motivating discussions of boolean functions and his patient reading of the manuscript. She is also indebted to D. AUGOT for helpful discussions on the use of Maple and to V. A. ZINOVIEV and P. SOLÉ for valuable references. She wishes to thank the referees for many useful remarks.

References

- [1] E.F. ASSMUS & V. PLESS *On the covering radius of extremal self-dual codes*, IEEE Trans. on Info. Theory, vol. IT-29, n. 3, May 1983.
- [2] L.A. BASSALYGO, G.V. ZAITSEV & V.A. ZINOVIEV, *Uniformly packed codes*, translated from Problemy Peredachi Informatsii, vol. 10, N. 1, pp. 9-14, January-March, 1974.
- [3] L.A. BASSALYGO & V.A. ZINOVIEV, *Remark on uniformly packed codes*, translated from Problemy Peredachi Informatsii, vol. 13, N. 3, pp. 22-25, July-September 1977.
- [4] T. BERGER, *The automorphism group of double-error-correcting BCH-code*, to appear in IEEE Trans on Info. Theory.
- [5] S.D. BERMAN, *On the theory of group codes*, KIBERNETICA, Vol. 1, n. 1, pp. 31-39, 1967.
- [6] A.E. BROUWER, A.M. COHEN & A. NEUMAIER, *Distance-regular Graphs*, Springer, Berlin 1989.
- [7] A.R. CALDERBANK & J.M. GÆTHALS, *On a pair of dual subschemes of the Hamming scheme $H_n(q)$* , Europ. J. Combinatorics, (1985) 6, 133-147.
- [8] P. CAMION, B. COURTEAU, G. FOURNIER & S.V. KANETKAR, *Weight distribution of translates of linear codes and generalized Pless Identities*, J. Inform. Optim. Sci. 8, 1-23 (1987).
- [9] P. CAMION, B. COURTEAU & A. MONTPETIT, *Weight distribution of 2-error correcting binary BCH codes of length 15, 63 and 255*, IEEE Trans. on Inform. Theory, vol. 38, No. 4, pp. 1353-1357, 1992.
- [10] P. CAMION, B. COURTEAU & P. DELSARTE, *On r -partition designs in Hamming spaces*, Applicable Algebra in Eng. Comm. and Computing 2, 147-162 (1992).
- [11] C. CARLET, *Codes de Reed et Muller, codes de Kerdock et de Preparata*, Thèse de l'Université Paris 6, Janvier 90.
- [12] P. CHARPIN, *Puissance du radical d'une algèbre modulaire et codes cycliques*, Revue du CETHEDC, 18ième année, NS81-2, pp 35-43.
- [13] P. CHARPIN, *Codes idéaux de certaines algèbres modulaires*, Thèse de Doctorat d'Etat, Université Paris 7, 1987.

- [14] P. CHARPIN, *Codes cycliques étendus affines-invariants et antichaines d'un ensemble partiellement ordonné*, Discrete Mathematics 80 (1990), 229-247.
- [15] P. CHARPIN, *Distributions de poids des translatés des codes BCH binaires 2-correcteurs*, C. R. Acad. des Sciences de Paris, t.317, Série I, p.975-980, 1993.
- [16] P. CHARPIN, *Tools for cosets weight enumerators of some codes*, submitted.
- [17] B. COURTEAU & A. MONTPETIT, *Dual distances of completely regular codes*, Discrete Mathematics 89 (1991), 7-15.
- [18] P. DELSARTE, *Four fundamental parameters of a code and their combinatorial significance*, Information and Control, vol. 23, N. 5, pp.407-438, 1973.
- [19] P. DELSARTE & J.M. GÆTHALS, *Irreducible binary cyclic codes of even dimension*, in: Combinatorial Mathematics and its Applications, Proc. Second Chapel Hill Conference, May 70 (Univ. of North Carolina, Chapel Hill, N.C.,1970) pp. 100-113.
- [20] J.M. GÆTHALS & H.C.A. VAN TILBORG, *Uniformly packed codes*, Philips Res. Repts 30, 9-36, 1975.
- [21] D.C. GORENSTEIN, W.W. PETERSON & N. ZIERLER, *Two-error correcting Bose-Chaudhuri codes are quasi-perfect*, Information and Control, 3(1960) 291-94.
- [22] T. KASAMI, *Weight distributions of Bose-Chaudhuri-Hocquenghem codes*, in: Proceedings of the conference on combinatorial mathematics and its applications (R.C. BOSE and T.A. DOWLING, EDS., The Univ. of North Carolina Press, Chapel Hill, N.C., 1968, pp. 335-357.
- [23] F.J. MACWILLIAMS & N.J.A. SLOANE, *The theory of Error Correcting Codes*, North-Holland 1986.
- [24] W.W. PETERSON, *On the weight structure and symmetry of BCH codes*, Scientific Report AFCRL-65-515, Air Force Cambridge Research Labs., Bedford, Mass., July 1965.
- [25] V. PLESS, *Power moment identities on weight distributions in error correcting codes*, Info. and Control, 6 (1963), 147-152.
- [26] N.V. SEMAKOV, V.A. ZINOVIEV & G.V. ZAITSEV, *Uniformly packed codes*, Problemy peredatshi informatsii (1971) 7, 1, 38-50.
- [27] H.C.A. VAN TILBORG, *Uniformly packed codes*, Ph.D. thesis, Tech. Univ. Eindhoven, 1976.
- [28] J. WOLFMANN *The number of points on certain algebraic curves over finite fields*, Communications in Algebra, 17(8), 2055-2060 (1989).

Numerical results

1. Cosets of the 2-error-correcting BCH-code of length 15 and of the extended code of length 16

The height weight enumerators of the cosets of the extended BCH-code, with parameters $[16, 7, 6]$, (by using Table 9) :

weights	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
weight distrib. of the 8 cosets	1						48		30		48						1
		1				18		45		45		18				1	
			1		6		31		52		31		6		1		
				1		21		42		42		21		1			
				3		15		46		46		15		3			
					8		32		48		32		8				
					4		48		24		48		4				
					12		16		72		16		12				

Applying Formula (25), we find again the height weight enumerators of the cosets of the BCH-code of parameters $[15, 7, 5]$, computed in [9]:

weights	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
weight distrib. of the 8 cosets	1					18	30	15	15	30	18					1
		1			6	12	19	26	26	19	12	6			1	
			1		6	15	16	26	26	16	15	6		1		
			1	2	4	11	20	26	26	20	11	4	2	1		
				1	7	14	18	24	24	18	14	7	1			
				3	5	10	22	24	24	22	10	5	3			
				1	3	18	30	12	12	30	18	3	1			
				3	9	6	10	36	36	10	6	9	3			

2. Cosets of the 2-error-correcting BCH-code of length 31 and of the extended code of length 32

The five weight enumerators of the cosets of the extended BCH-code, with parameters $[32, 21, 6]$, (by using Table 8) :

weights	The five cosets				
0, 32	1				
1, 31		1			
2, 30			1		
3, 29				5	
4, 28			30		40
5, 27		186		197	
6, 26	992		907		864
7, 25		3441		3282	
8, 24	10540		10220		10320
9, 23		26815		27410	
10, 22	60512		63065		62944
11, 21		127162		125963	
12, 20	228160		220482		220504
13, 19		337900		339275	
14, 18	446400		460315		460480
15, 17		553071		552444	
16	603942		587112		586848

Applying Formula (25), we find the four weight enumerators of the cosets of the BCH-code of parameters $[31, 21, 5]$,

weights	The four cosets			
0, 31	1			
1, 30		1		
2, 29			1	
3, 28			4	5
4, 27		30	26	35
5, 26	186	156	171	162
6, 25	806	751	736	702
7, 24	2635	2690	2546	2580
8, 23	7905	7530	7674	7740
9, 22	18910	19285	19736	19670
10, 21	41602	43780	43329	43274
11, 20	85560	83382	82634	82689
12, 19	142600	137100	137848	137815
13, 18	195300	200800	201427	201460
14, 17	251100	259515	258888	259020
15, 16	301971	293556	293556	293424

3. Distance matrices of 2-error-correcting BCH-codes and of its extension. for the length $2^m - 1$, m even.

When m is odd, it is very easy to compute the distance matrices, by means of the formula given in Section 5. So we only give the distance matrices of B and \hat{B} for small even values of m . We use the formal expressions given in Section 5.

3.1. $m = 6$ (we find again the matrix B which was computed in [9]).

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1890 \\ 0 & 1 & 0 & 0 & 150 & 1740 \\ 0 & 0 & 1 & 12 & 138 & 1683 \\ 0 & 0 & 1 & 8 & 142 & 1739 \\ 0 & 0 & 0 & 13 & 147 & 1674 \\ 0 & 0 & 0 & 9 & 151 & 1730 \\ 0 & 0 & 0 & 13 & 195 & 1626 \\ 0 & 0 & 0 & 9 & 135 & 1746 \end{bmatrix} \quad \hat{B} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 20160 \\ 0 & 1 & 0 & 0 & 0 & 1890 & 0 \\ 0 & 0 & 1 & 0 & 150 & 0 & 18307 \\ 0 & 0 & 0 & 13 & 0 & 1821 & 0 \\ 0 & 0 & 0 & 9 & 0 & 1881 & 0 \\ 0 & 0 & 0 & 0 & 160 & 0 & 18304 \\ 0 & 0 & 0 & 0 & 208 & 0 & 17344 \\ 0 & 0 & 0 & 0 & 144 & 0 & 18624 \end{bmatrix}$$

3.2. $m = 8$ (we find again the matrix B which was computed in [9]).

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 134946 \\ 0 & 1 & 0 & 0 & 2646 & 132300 \\ 0 & 0 & 1 & 36 & 2610 & 132147 \\ 0 & 0 & 1 & 44 & 2602 & 131651 \\ 0 & 0 & 0 & 37 & 2651 & 132106 \\ 0 & 0 & 0 & 45 & 2643 & 131610 \\ 0 & 0 & 0 & 37 & 2331 & 132426 \\ 0 & 0 & 0 & 45 & 2835 & 131418 \end{bmatrix} \quad \hat{B} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 5757696 \\ 0 & 1 & 0 & 0 & 0 & 134946 & 0 \\ 0 & 0 & 1 & 0 & 2646 & 0 & 5623443 \\ 0 & 0 & 0 & 37 & 0 & 134757 & 0 \\ 0 & 0 & 0 & 45 & 0 & 134253 & 0 \\ 0 & 0 & 0 & 0 & 2688 & 0 & 5623296 \\ 0 & 0 & 0 & 0 & 2368 & 0 & 5650176 \\ 0 & 0 & 0 & 0 & 2880 & 0 & 5607168 \end{bmatrix}$$

3.3. $m = 10$.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 8869410 \\ 0 & 1 & 0 & 0 & 43350 & 8826060 \\ 0 & 0 & 1 & 180 & 43170 & 8814867 \\ 0 & 0 & 1 & 164 & 43186 & 8818931 \\ 0 & 0 & 0 & 181 & 43339 & 8814698 \\ 0 & 0 & 0 & 165 & 43355 & 8818762 \\ 0 & 0 & 0 & 181 & 46155 & 8811882 \\ 0 & 0 & 0 & 165 & 42075 & 8820042 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1513712640 \\ 0 & 1 & 0 & 0 & 0 & 8869410 & 0 \\ 0 & 0 & 1 & 0 & 43350 & 0 & 1504854739 \\ 0 & 0 & 0 & 181 & 0 & 8858037 & 0 \\ 0 & 0 & 0 & 165 & 0 & 8862117 & 0 \\ 0 & 0 & 0 & 0 & 43520 & 0 & 1504851968 \\ 0 & 0 & 0 & 0 & 46336 & 0 & 1503894528 \\ 0 & 0 & 0 & 0 & 42240 & 0 & 1505287168 \end{bmatrix}$$

3.4. $m = 12$.

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 571404834 \\ 0 & 1 & 0 & 0 & 697686 & 570707148 \\ 0 & 0 & 1 & 660 & 697026 & 570590163 \\ 0 & 0 & 1 & 692 & 696994 & 570557459 \\ 0 & 0 & 0 & 661 & 697707 & 570589482 \\ 0 & 0 & 0 & 693 & 697675 & 570556778 \\ 0 & 0 & 0 & 661 & 676203 & 570610986 \\ 0 & 0 & 0 & 693 & 708939 & 570545514 \end{bmatrix}$$

$$\hat{B} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 390079033344 \\ 0 & 1 & 0 & 0 & 0 & 571404834 & 0 \\ 0 & 0 & 1 & 0 & 697686 & 0 & 389507814355 \\ 0 & 0 & 0 & 661 & 0 & 571287189 & 0 \\ 0 & 0 & 0 & 693 & 0 & 571254453 & 0 \\ 0 & 0 & 0 & 0 & 698368 & 0 & 389507768320 \\ 0 & 0 & 0 & 0 & 676864 & 0 & 389537099776 \\ 0 & 0 & 0 & 0 & 709632 & 0 & 389492404224 \end{bmatrix}$$



Unité de Recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 LE CHESNAY Cedex (France)
Unité de Recherche INRIA Lorraine Technopôle de Nancy-Brabois - Campus Scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 VILLERS LES NANCY Cedex (France)
Unité de Recherche INRIA Rennes IRISA, Campus Universitaire de Beaulieu 35042 RENNES Cedex (France)
Unité de Recherche INRIA Rhône-Alpes 46, avenue Félix Viallet - 38031 GRENOBLE Cedex (France)
Unité de Recherche INRIA Sophia Antipolis 2004, route des Lucioles - B.P. 93 - 06902 SOPHIA ANTIPOLIS Cedex (France)

EDITEUR
INRIA - Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 LE CHESNAY Cedex (France)

ISSN 0249 - 6399



★ R R - 2 2 2 8 ★